Proceedings of the 2\textsuperscript{nd} International Scientific Conference of Cihan University-Erbil on Communication Engineering and Computer Science

(CIC-COCOS’17)

March 29-30, 2017
Cihan University-Erbil, Kurdistan Region-Iraq

ISSN: 2520-4777
The Conference Secretariat mailing address:
Research Center
Cihan University-Erbil,
100m Street, Nawroz Qr.,
44001, Erbil
Iraq
Phone +964 751 7688597
Email: cic@cihanuniversity.edu.iq
ISSN : 2520-4777
Copyright © 2017. All rights reserved to Cihan University-Erbil
A message from Chairman of Board of the Trustees of Cihan Group Universities

By the name of board of trustees, I would like to welcome all to Cihan University Second International Conference on Communication Engineering and Computer Sciences. I would like to express my deep gratitude to the keynotes, researchers, and all participants for their efforts in participating in this conference which enrich the academic process for our university and serve the society and all humanity since researches are the main pillar of building and improving high ranked and distinguished universities. These researches would be highly appreciated and considered not only by the university itself but even more by the society and other institutions of the same field. We aim at sharing global knowledge and experience to achieve better service to our community through such valuable papers.

I, as the Chairman of Board of Trustees, offer all the modern and technological facilities to achieve a high quality of teaching, learning, and researching.

I am very thankful to Cihan University staff members, the organizing committee, and all participants to arrange for this Conference who did a lot to make it happen.

Dr. Nawzad Bajger
Chairman of Board of the Trustees of Cihan Group Universities
A message from President of Cihan University-Erbil

I am greatly honored and pleased to welcome you all to Cihan University International Conference on Communication Engineering and Computer Science (CIC-COCOS'17). I would like to declare that the 2nd international conference is now open. As we open this conference, I would like to express my gratitude and a warm welcoming to our keynote speakers as well as the presenters, especially those who are coming from overseas.

Academic research and the education of talented individuals are two goals unique to universities, Cihan University has been recognized in offering support and opportunities for students and staff to acquire knowledge and experience for the professional life. Furthermore, the National University Ranking (NUR) introduced by the Ministry of Higher Education and Scientific Research and the most recent changes in NUR that places a much higher emphasis on internationalization and research output has become the annual national benchmark universities use to ascertain their relative standing in the region.

In response, in 2016-2017 Cihan University has adopted the strategy of hosting discipline-specific international conferences and inviting international scholars in Science, Engineering and Humanities and Social Sciences.

The aim of these conferences is to share in the global research output activities, capacity building through information sharing, and to renew contacts and discuss problems of mutual interest with international academics from member countries of the region.

I am most thankful to all organizers and staff members at Cihan University and I wish you all a wonderful time of interaction and learning from a host of presentation and fellow attendees.

Asst. Prof. Dr. Fuad Mawlood Shareef
President of Cihan University-Erbil
Preface

This volume of Conference Proceedings contains the written versions of the contributions presented during the 2nd International Scientific Conference of Cihan University-Erbil on Communication Engineering and Computer Sciences that took place at the Cihan University-Erbil campus from March 29–30, 2017. The Conference provided a setting for discussing recent developments in a wide variety of topics in communication engineering and computer sciences. The Conference has been a good opportunity for participants to present and discuss topics in their respective research areas. The scientific program consisted of two plenary sessions and eight parallel sessions.

I would like to thank all participants for their contributions to the conference program and for their contributions to these proceedings. I also acknowledge the reviewers for their detailed comments and suggestions for the submitted papers. We believe that the comments have identified important areas which required improvements of the contents. I would also like to show my appreciation for the keynote speakers for their efforts that made a great contribution to the success of the conference. My special thanks go to our colleagues for their devoted assistance in the overall organization of the conference. Many thanks to the Cihan University-Erbil Presidency for their support and hospitality. It is my pleasant duty to acknowledge the financial support from the Board of the Trustees of Cihan Group Universities. Without their support the conference organization could not have been as successful as it was.

The continuing success of this conference series means that planning can now proceed with confidence for the next International Conference of Cihan University-Erbil on Communication Engineering and Computer Sciences which we are looking forward to hold in 2018. I hope that it will be an interesting and a beneficial conference.

Conference General Chair
CIC-COCOS’17 ORGANIZATION COMMITTEES

Honorary Chair: Asst. Prof. Dr. Fuad M. Shareef 
(President of Cihan University-Erbil)

Honorary Co-Chair: Asst. Prof. Dr. Nejdet Z. Shakir 
(Deputy President of Cihan University-Erbil for Scientific Affairs)

General Chair: Prof. Dr. Mohammad Abdulbaqy 
(Director of Research Center of Cihan University-Erbil)

Scientific Committee

Dr. Husham J. A. Alqaysi (Chair)
Departement of Communication and Computer Engineering
Cihan University-Erbil

Asst. Prof. Dr. Samah A. Mustafa
Department of Electrical Engineering
Salahaddin University-Erbil

Dr. Salim Muhammad Zaki
Departement of Computer Sciences
Cihan University-Erbil

Dr. Reem Jafar Ismail
Departement of Computer Sciences
Cihan University-Erbil

Dr. Laith R. Fliah
Departement of Computer Sciences
Cihan University-Erbil
Dr. Abdulqadir Ismaïl Khoshnaw  
Departement of Communication and Computer Engineering  
Cihan University-Erbil

Dr. Jalal Jamal Hamadamin  
Department of Electrical Engineering  
Salahaddin University-Erbil

Dr. Moayad Yousif Potrus  
Department of Software Engineering  
Salahaddin University-Erbil

Dr. Rasber Dhahir Rasheed  
Department of Software Engineering  
Koya University

Logistic Committee  
Asst. Prof. Dr. Sabah Subhi (Chair)  
Dr. Mahsa Mishfiqyan  
Mr. Adnan Jameel Mukhlif  
Mr. Ibrahim Othman Ali

Secretariat Committee  
Mrs. Mardin A. Anwer (Chair)  
Mr. Ali Nuraddin Ahmed  
Ms. Shoxan Star Sadiq
**IT Committee**
Mr. Mohammed Hussein Shukur (Chair)
   Mr. Mohamad T. Sultan
   Mr. Omar Talal Hamid

**Publishing Committee**
Dr. Mohammad Khidir (Chair)
Mr. Hawjhin Omar Mohammad
Mr. Abeer Mahmood Jabbar
Ms. Ashna Anwar Kareem

**Social Activities Committee**
Mr. Hunar Mohammad Hussain (Chair)
   Mr. Xanda Sarkawt Othman
   Ms. Hamsa Khalil Ali

**Financial Committee**
Mr. Hiwa Omar Ali
Mr. Ferhang Saman Mustafa
CIC-COCOS’17 KEYNOTE SPEAKERS
Prof. Dr. Sabah A. Jassim

Prof. Dr. Sabah Jassim is received the B.Sc. and M.Sc. degrees both in mathematics from Baghdad University, Baghdad, Iraq, and received the Ph.D. degree in mathematics from the University of Wales-Swansea, Swansea, U.K. His academic career includes various lecturing posts at a number of U.K. and international institutions including University of Wales, Swansea; City University, London; De Montfort University (formerly Leicester Polytechnic); and Fachhochschule Wedel, Germany. In 1989, he joined the University of Buckingham, Buckingham, U.K., where he is currently a Professor of mathematics, and the Head of Applied Computing Department. His research interest includes multimodal and multistream biometrics authentication, revocable biometric cryptosystems, security of multimedia objects, environment aware adaptive face recognition, computational geometry and graph algorithms, bioinformatics and pathway analysis, wavelet-base image/video processing/analysis, compression and indexing, and visual speech/word recognition.
Assoc. Prof. Dr. Jaime Lloret Mauri

Assoc. Prof. Dr. Jaime Lloret received his M.Sc. in Physics in 1997 at University of Valencia and he finished a postgraduate Master in Corporative networks and Systems Integration from the Department of Communications in 1999. Later, he received his M.Sc. in Electronic Engineering in 2003 at University of Valencia and his Ph.D. in telecommunication engineering (Dr. Ing.) at the Polytechnic University of Valencia in 2006. Before concluding his PhD. Thesis he obtained the first place given by the Spanish Agency for Quality Assessment and Accreditation for the Campus of Excellence in the New Technologies and Applied Sciences Area. He was awarded the prize of the best doctoral Student in the Telecommunications area in 2006 according to the Social Council of the Polytechnic University of Valencia. He is a Cisco Certified Network Professional Instructor of the regional academy "Universidad Politécnica de Valencia" in the Cisco Networking Academy Program (CNAP) and he is the Legal Main Contact of UPV-ADIF (local academy of the CNAP). He teaches Local Area Networks and Systems Integration in the "Escuela Politecnica Superior de Gandia" from the Polytechnic University of Valencia. He has been working as a network designer and administrator in several companies. His academic interests and research are P2P networks, Wireless Local Area Networks, Sensor Networks and Routing Protocols. He also researches on educational approaches and strategies.
# Table of Contents

<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iraqi Car License Plate Recognition Using OCR</td>
<td>1-6</td>
</tr>
<tr>
<td><em>Safaa S. Omran &amp; Jamana A. Jarallah</em></td>
<td></td>
</tr>
<tr>
<td>Comparative Study of Reconfigurable Cache Memory</td>
<td>7-13</td>
</tr>
<tr>
<td><em>Safaa S. Omran &amp; Ibrahim A. Amory</em></td>
<td></td>
</tr>
<tr>
<td>Design SHA-2 MIPS Processor Using FPGA</td>
<td>14-18</td>
</tr>
<tr>
<td><em>Safaa S. Omran &amp; Laith F. Jumma</em></td>
<td></td>
</tr>
<tr>
<td>A comparative analysis between low and high level HoneyPots</td>
<td>19-23</td>
</tr>
<tr>
<td><em>Rebin B. Khoshnaw</em></td>
<td></td>
</tr>
<tr>
<td>Comparative Study for Color Edge Detection Using Vector Value, YCbCr Color Space and Least Square Numerical Method</td>
<td>24-29</td>
</tr>
<tr>
<td><em>Sarah Behnam Aziz, Dalya Abdullah Anwer &amp; Mardin A. Anwer</em></td>
<td></td>
</tr>
<tr>
<td>Designing An Efficient Three Phase Brushless DC Motor Fuzzy Control Systems (BLDCM)</td>
<td>30-35</td>
</tr>
<tr>
<td><em>Rafid Ali Ridha Ibrahim &amp; Inas Bahaa Abedalrazzaq Deabil</em></td>
<td></td>
</tr>
<tr>
<td><em>Mohamad T. Sultan &amp; Salim M. Zaki</em></td>
<td></td>
</tr>
<tr>
<td>Study and Analysis of Students’ Works after Graduation from Computer Science Department in Cihan University – Erbil</td>
<td>40-44</td>
</tr>
<tr>
<td><em>Reem Jafar Ismail &amp; Omar Talal Hamid</em></td>
<td></td>
</tr>
<tr>
<td>Factors influencing the adoption of Location Based Identification in Kurdistan Regional of Iraq</td>
<td>45-51</td>
</tr>
<tr>
<td><em>Sara Muhamad Amin</em></td>
<td></td>
</tr>
<tr>
<td>Challenges Smartphone’s Big Data in HealthCare Systems</td>
<td>52-54</td>
</tr>
<tr>
<td><em>Mohammed Hussein Shukur, Laith R. Fliah and Aram Mohammed</em></td>
<td></td>
</tr>
<tr>
<td>Analysis of Confidentiality Algorithms in Different Mobile Generations</td>
<td>55-61</td>
</tr>
<tr>
<td><em>Khalid Fadhil Jasim &amp; Imad Fakhri Al-Shaikhli</em></td>
<td></td>
</tr>
<tr>
<td>Comprehensive Study of Hierarchical Routing Protocols in MANET using Simple Clustering</td>
<td>62-65</td>
</tr>
<tr>
<td><em>Ghassan A. QasMarrogy, Husham J. A. Alqaysi &amp; Yazen S. Almashhadani</em></td>
<td></td>
</tr>
<tr>
<td>Performance Analysis of OFDM with Different Cyclic Prefix Length</td>
<td>66-69</td>
</tr>
<tr>
<td><em>Yazen S. Almashhadani, Husham J. A. Alqaysi &amp; Ghassan A. QasMarrogy</em></td>
<td></td>
</tr>
<tr>
<td>Development of an IoT-based Noise Monitoring Network</td>
<td>70-74</td>
</tr>
<tr>
<td><em>Aram Mohammad Abdulqadir &amp; Mohammed Hussein Shukur</em></td>
<td></td>
</tr>
</tbody>
</table>
Satellite Link Budget Calculator by Using Matlab/GUI
Adil Hussein M. Al-Dalowi, Abdulqadir Ismail Khoshnaw & Ghassan A. QasMarrogy

Enhanced Situational Awareness and Security Assessment in Surveillance Systems Using Cloud Model Theory
Abdulqadir Ismail Khoshnaw, Adil Hussain M. Al-Dalowi & Ghassan A. QasMarrogy

Database Protection System Depend on Modified Hash Function
Alaa K. Farhan & Mohammed Abed Al-jabber Ali

The Impact of Information Security International Standards
Thabit H. Thabit & Yaser A. Jasim

PerfectC2MIS: A perfect FileMaker r-database based comprehensive Class cum Course Management Information System
Atul Sharma & Omead Ibraheem Hussain
Iraqi Car License Plate Recognition Using OCR

Safaa S. Omran  
Computer Engineering Techniques College of  
Electrical and Electronic Techniques Baghdad,  
Iraq  
omran_safaa@ymail.com

Jumana A. Jarallah  
Computer Engineering Techniques College of  
Electrical and Electronic Techniques Baghdad,  
Iraq  
jumanaabdulhadi@yahoo.com

DOI: 10.24086/cocos17.19

Abstract— License plate recognition (LPR) system is an important system in our life. LPR is an image processing and a character recognition system that used to recognize any car from the others. An automatic license plate recognition system for Iraqi car license plates is proposed in this paper. An optical character recognition (OCR) is used with correlation approach and templates matching for plate recognition in this system. The software used is MATLAB R2014a. The algorithm is successfully constructed with sample of images correctly identified.

Keywords— license plate recognition, optical character recognition, image processing, correlation, Otsu's thresholding, tophat filtering.

I. INTRODUCTION

A License Plate (LP) is a rectangular metal plate contains numbers, characters and words, fixed on the car body and is used to identify the vehicles. In recent years, the importance of recognizing LP characters and numerals in an automatic manner has largely increased [1]. This research aims to recognize the numerals and characters, extracted from Iraqi LPs, into a text.

The recognition of license plates is very important in many applications such as Parking, Borders control, Detect and monitor traffic, Travel and Airport parking [2].

In many countries the license plates that written in English language as samples shown in Fig.1, the English letters is separated and the LP have a similar design for all cities in the country, so that will facilitate the recognition process of the characters. Because the LP is different and specific for each country, so the algorithms used for LPR system is different and specific too.

In Iraq, there are 3 styles for Iraqi car license plates written in Arabic language [1] [3]. The first style is for the three Northern provinces (Erbil, Sulymania and Duhok) as shown in Fig.2a the second style is the old style (before 2003) as shown in Fig.2b, and the third style is the new style which is shown in Fig.2c. The second and third styles are used for the other fifteen provinces and each has a different size and design.

Fig. 2. Iraqi car license plate types

a. Northern provinces style
b. Old style
c. New style

This research mainly consists of the following parts:

1) Location plate part or license plate detection (LPD): Is the first part of the system where locating the license plate from the car image.
2) Distinguishing between the three styles of Iraqi LP: in this part the differentiation between the three styles of Iraqi license plates is take place.
3) Pre-processing part: Thresholding using Otsu's method and morphological operations to enhance LP image.
4) License plate character segmentation (LPCS): Segment each number, character and word into sub images.
5) OCR part: Optical character recognition method for numbers, characters and words recognition.

Ng Simin [4] proposed Automatic car plate detection and recognition system for Malaysian car number plates, the algorithm constructed is to target field programmable gate

This paper is organized as follows: The algorithm used to implement the LPR system is described in section II and Experimental results are described in section III. Finally, Conclusion is summarized in Section IV.

II. LPR SYSTEM ALGORITHM

The main stages of the proposed system shown in Fig.3, these stages are:

A. Car image acquisition

This is the first and the primary stage in LPR, the aim of it is to capture the front or the back side of the car where the license plate usually placed then applies the captured image to the next stage of the system. In this system the front side of the car is chosen and the database images are collected from many places like my college, parks and streets as shown in Fig.4.

B. Locating the LP from the car image

After the picture is captured the system works to locate the LP from the car image. In this stage the first step is cutting and resizing the original image as shown in Fig.5b. Then Image processing performed to focus the area of number plate [11], Smooth edges and contours to delete characters as shown in Fig.5c, Subtracting the original image to obtain the information previously deleted using tophat filtering and thus stays with the characters as shown in Fig.5d. Then removing the related elements with less than 70 pixels, Remove objects that are not candidates for plate and select the largest connected component after preprocessing as shown in Fig.5e, then cutting the plate from the original image as shown in Fig.5f.

C. Distinguish between the three styles of Iraqi LP

After the plate position was located, in this step the distinguishing between the three styles of the LP is taken place. The basic step used in discrimination between the three styles of the Iraqi LP is from the size of the plate. The flowchart in Fig. 6 describes how to detect the size of the plate to discriminate between the three styles.

Fig. 4 Captured images
If any of the three styles of LP was found, the process of the recognition will follow the process shown in Fig.7 with some differences explained later in each stage.

![Flowchart for distinguishing between the three styles of Iraqi LP](image)

**D. Binarization**

After distinguishing between the three styles of the license plates, it is the time of converting the gray image (gray LP image from the locating LP stage) to a binary image as shown in Fig.8a and this is done by using Otsu's thresholding [12], it is used to automatically perform clustering based image thresholding, or the reduction of a gray level image to a binary image. The algorithm of this method calculates the optimum threshold separating the two classes (foreground and background).

The pseudo-code can be translated in MATLAB such as using the two following instructions:

```
level = graythresh(I) %find the optimum threshold for the image.
BW = im2bw(I, level); %convert image to binary based on level.
```

Afterwards, complement of binary image takes place as shown in Fig.8b, because the background of the image is white and the foreground is black and the required is opposite to perform the recognition correctly.
OCR is the process of converting an image into a computer editable text. The text and numbers in an image is not editable, the letters, characters and numbers are made of tiny dots (pixels) that together form a picture of text and numbers. OCR is classified into two types, offline recognition and online recognition. In offline recognition the source is either an image or a scanned form of the document whereas in online recognition the successive points are represented as a function of time and the order of strokes are also available. Here in this paper only offline recognition is used [4][13].

In this stage, first the numbers are segmented (each number into sub-image) by using labeling connected components [9] as shown in Fig.11. Each number, letter, province and type should be resized to the size of the preloaded templates.

Images of numbers from 0 to 9, Iraq provinces, letters and types of cars in Iraqi LP all these variables are stored in the form of cell in which each matrix represents a character, all the model inputs are saved under the name 'TEMPLATES'. The separated images of numbers, letters, provinces and type are correlated with templates (each part with its saved templates) which are reloaded into the system. Once the correlation is completed, the template with the maximum correlated value is declared as the character present in the image and prints it into a text file.

In the new style of the LP there is a difference in the type and province recognition. Before the dividing process of the type and province, first cutting the type and province together to decide if the car type is government or not. This is done by counting the number of labeling connected components objects. If the number of objects is less than or equal to five then the car type is government, else the dividing process and recognition for type and province is taking place as shown in Fig.12. This procedure were required because the government LP has only one word (حكومية) while the other LPs have two words as shown in Table II.
There are 30 from total 35 images that the LP extracted the recognition is correct, the 5 images are correctly extracted the LP but the recognition failed, that because the LP is not divided correctly in the dividing stage to preparing the LP for recognition stage. For example, in the number part there are more objects not the numbers only that makes the recognition process failed as shown in Fig.14.

![Incorrect dividing](image14)

The results of the recognition for some samples of cars are given by Table II.

TABLE II. EXPERIMENTAL RESULTS OF RECOGNITION

<table>
<thead>
<tr>
<th>Car image</th>
<th>Image plate</th>
<th>Results (text file)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image22" alt="Car image" /></td>
<td><img src="image23" alt="Image plate" /></td>
<td><img src="image24" alt="Results (text file)" /></td>
</tr>
</tbody>
</table>

![Incorrect crop of LP](image13)

The database that used to test the system is 40 images, only 35 LP are extracted correctly. The main reasons that the 5 images are not extracted are: either image is unclear or the process of clean up the unwanted objects in some images will wiped out some important information and that cause the crop of the LP is incorrect as shown in Fig.13.

![Incorrect crop of LP](image13)
IV. CONCLUSION

In this paper, the application software for the recognition of car license plate is designed. Firstly we extracted the plate location, and then separate the plate characters individually by segmentation and finally applying template matching with the use of correlation for recognition of plate characters. This system is designed for the identification for Iraqi license plates and the system is tested over a 40 images. Finally it is proved to be 87.5% for extraction of plate region and 85.7% for the recognition unit accurate, giving the overall system performance of 86.6% recognition rate.

REFERENCES


Comparative Study of Reconfigurable Cache Memory

Safaa S. Omran
Department of Computer Engineering
College of Electrical and Electronic Engineering Techniques
Baghdad, Iraq
Omran_safaa@ymail.com

Ibrahim A. Amory
Department of Computer Engineering
College of Electrical and Electronic Engineering Techniques
Baghdad, Iraq
Ibrahim_a7@yahoo.com

DOI: 10.24086/cocos17.01

Abstract—Reconfigurable cache memory is important to improve the cache performance and reduces the energy consumption. In this paper, a review for previous papers related with reconfigurable cache memory were presented and compared it with our work in which we implemented two dimensional reconfigurable cache memory with exploitation of full amount of cache memory size with different organizations and compare the performance of different cache organizations.

Keywords—Reconfigurable Cache; Hit ratio; Energy consumption; SRAM; FPGA.

I. INTRODUCTION

The modern microprocessors performance depends on the processing speed and the energy saving feature. The cache memory is placed between the CPU and main memory and it represents important part because it reduces the speed gap between CPU (Central Processor Unit) and RAM (Random Access Memory). The cache memory prefetching the data from the main memory before the processor request for it, that occurs with phenomenon known as locality of reference and there are two principles of locality: (spatial locality) and (temporal locality). The spatial locality principle states that programs tend to access data and instructions sequentially, and temporal locality refers to the tendency of programs to repeatedly use a small part of code/data over a certain time [1].

Power consumption has become a major design consideration. The cache memory consume about 50% of a microprocessor's energy. The performance of cache memory is approximately determined by specific applications. Better energy performance is achieved by different applications with different configuration of the cache memory. Several solutions have been proposed to reduce the energy consumption of the cache memory.

II. COMPREHENSIVE STUDIES

A selective cache ways proposed by David H. Albonesi [2] exploits the fact that large on-chip caches are often partitioned into multiple sub arrays to reduce the long word delays of a single large array. This is for the data array and for set associative caches for which the word lines can be exceedingly long.

The partitioning required to combine hardware and software elements. A partitioning of the data and tag arrays into one or more subarrays for each cache way. Also a gating hardware and decision logic for disabling the operation of particular ways. Design a cache way select register as a software-visible register that signals the hardware to enable/disable particular ways.

Fig. 1 shows the 4 way set associative cache using selective cache ways.

![Figure 1. 4-way Set Associative Cache using Selective Cache ways.](image)

One advantage of selective cache ways over static solutions to energy reduction is that the tradeoff between performance and energy dissipation can be made variable via different Performance Degradation Threshold values.
The results shown that for the 4-way set associative caches, performance degrades by 0-4% when only three ways are enabled, and more sharply thereafter. The degradation is particularly significant (up to 17%) when moving from two ways to only one way enabled.

This is also the case for the 2-way set associative caches, in which performance degrades by 2-11% when only one of the two ways is enabled.

The energy savings for 2-way set associative caches is significantly less than that of 4-way caches of the same size for two reasons. First, a large jump in conflict misses often accompanies a move from two ways to only one way enabled. Second, the higher granularity of partitioning in the 4-way caches allows for the potential of disabling a greater percentage of the cache. Thus, in general, the effectiveness of selective cache ways increases with the cache associativity.

A 40% reduction in overall cache energy dissipation can be achieved for 4-way set associative caches with less than a 2% overall performance degradation.

A reconfigurable cache design proposed by Ranganathan et al. [3] enables the cache SRAM arrays to be dynamically divided into multiple partitions that can be used for different processor activities.

They divide the reconfigurable cache into partitions at the granularity of the ways of the conventional cache, exploiting the conceptual division into ways already present in a conventional cache.

A reconfigurable cache will require an equal or greater number of subarrays than a non-reconfigurable cache.

An increase in the number of subarrays can have two effects: if the number of subarrays is larger, the wire area and delay required to connect them will be larger, and a larger number of subarrays results in a reduction in the number of bits in each subarray, which means the individual subarray access times are reduced.

Their results show that a reconfigurable cache organization can increase the cache access time by anywhere between 1% to 15%. For small numbers of partitions (2-way), reconfigurable caches usually increase the access time of the non-configurable baseline cache by less than 5% (4% for a 128KB cache and 1% for a 1MB cache).

For larger numbers of partitions (4-way and 8-way), reconfigurable caches suffer a relatively larger cache access time penalty, particularly for smaller cache sizes (7-15% for the 128KB cache and 2-6% for the 1MB cache).

Zhang et al. [4] proposed way-concatenation depending on the associativity it can reduce dynamic power by accessing fewer ways. This was performed before an application started execution.

They choose to use a base cache of 8 Kbytes having four way set-associativity and a line size of 32 bytes. The base cache is the cache that they extend to be configurable.

A direct mapped cache has a high miss rate, resulting in higher energy due to longer time as well as high power for accessing the next level memory. Increasing cache associativity can decrease the cache miss rate and hence reduce energy.

Although accessing a four-way set associative cache requires more power per access, that extra power may be compensated for by the reduction in time and power that would have been caused by misses.

Fig. 2 shows the miss rate and normalized energy for 8 Kbyte data cache with different associativity.

They used two single-bit registers reg0 and reg1 that can be set to configure the cache as four, two or one way associative. Those two bits are combined with address bits a11 and a12 in a configuration circuit to generate four signals c0, c1, c2, c3, which are in turn used to control the configuration of the four ways.

Their results show a way-concatenatable cache results in an average energy savings of 37% compared to a conventional four-way cache, with savings over 60% for several examples. Compared to a conventional direct mapped cache, the average savings are more modest, but the direct mapped cache suffers large penalties for some examples – up to 284% for parser, with degraded performance in several examples.

Santana Gil et al. [5] proposed a design for reconfigurable cache with fixed size, the cache design can work as direct
mapped cache or as 2 way set associative cache, and can select 1, 2, 4 or 8 words per block for each mode.

The core of the reconfiguration mechanism is the Control Block. The Control Block is a pure combinational circuit. Once the working mode is selected, the reconfiguration process with no latency. Then, the cache is ready to work in the new selected mode at the next memory access.

The Control Block indicates if the cache operation resulted in a hit or a miss and proceeds controlling all processor buses, to provide data from cache or system RAM, according to the operation result.

They design a data cache memory of 2 K words of 32 bits (8 KB). Additional amount of memory is required to store the tags, valid bits and LRU bits.

The design was implemented on a Xilinx Spartan 3 starter board with a xc3s200-ft256 FPGA. The cache structure was described using Handel-C as a hardware description language.

Sundararajan et al. [6] presented a Set and Way management cache architecture for Run-Time reconfiguration that allows to change the size and associativity. The associativity can be selected as (Direct Mapped (DM), 2 Way and 4 Way) with sizes (64KB, 128KB, 256KB, 512K Byte, 1M Byte and 2M Byte).

They designed a cache memory with set selection and group the sets in each bank by augmenting the cache with size selection bits that determine the sets that are enabled. And the size selection bits then ANDed with bits from the index to determine the sets to access.

The five size selected bits representing cache size of 128KB, 256KB, 512KB, 1MB and 2MB. The 64KB cache is always enabled.

A way selection circuits control the associativity of the cache and it could be Direct Mapped (one way), 2 way and 4 way set associative.

Fig. 3 shows the accessed, unaccessed and disabled sets for each case of cache associativities.

![Figure 3. The smart cache. Brown, yellow and white regions show accessed, unaccessed and disabled sets respectively.](image)

The differences between this Smart cache and other reconfiguration techniques. The associativity and size are varied in parallel by using the way control signals and the size control registers. The Smart cache organizes ways at set boundaries, which avoids flushing data back to memory when increasing the associativity but keeping the cache size fixed.

They implemented cache reconfiguration using the HotLeakage simulator.

Their results shows that for some benchmarks the best static configuration is 2MB with eight-way associativity so there are no energy savings achievable for any cache architecture. The set-only, set-and-way and Smart approaches consume around 1.7% more energy compared to way-concatenation.

For other some benchmarks, the set-only and set-and-way approaches do not do well compared to the way-concatenation and Smart caches. The reason for this is that these benchmarks require a 2MB cache with two-way associativity which is only offered by way-concatenation and Smart cache. For these architectures, dynamic energy is reduced by accessing fewer ways, which is not possible in the set-only and set-and-way caches.

The average cache energy delay is 0.28, which is 14% better than set-only and set-and-way approaches and 25% better than the way-concatenation with way-shutdown approach. This clearly demonstrates the benefits of using their smart cache reconfiguration architecture.

Zhenglin Liu et al. [7] presented an efficient reconfiguration management algorithm (RMA) to improve the performance and energy-efficiency of the memory hierarchy.

They have described the differences between the variation in the energy consumption and the variation in the performance for different cache configurations. It is this difference in the variation that motivated to develop the RMA.

They used cache capacities of 4, 8, 16, 32, 64, and 128KB, associativities of 1, 2, 4 and 8-way, and line sizes of 16 and 32 Bytes. The total cache capacity has the biggest average impact on energy and miss rate, line size has little impact for instruction cache, but more impact for data cache because of spatial locality, and associativity has least impact among the three.

They refer to the method of overlapped wide-tag partitioning, which enables the cache partitions to potentially be any size, however, they limit them to be powers of two to enable simpler decoding. Because of 6 choices for the cache capacity. Thus, it is reasonable to physically partition the 128KB cache into 6 subarrays: 8KB, 16KB, 32KB and 64KB for each subarray, and 4KB for two subarrays.

The cache memory have “physical line” 8 Bytes, but to fetch and replace a variable number of words simultaneously as a “virtual line”. Besides, the approach allows the line size to be changed dynamically. They added a counter to cache controller to specify how many words to read from the off-
chip memory, and determine how many cache physical lines will be filled when there is a miss.

They utilize an 8-way set-associativity cache as baseline architecture and each way is enabled by one of the Cache Way Enable Signals using some decision logic and gating hardware. When a Way is disabled, no data is selected from a disabled way and its data array dissipates essentially no dynamic power.

Their results shows the cache of lowest energy dissipation is 32K8W64B with miss rate 0.0118 and energy dissipation 34.159nJ, however, the “optimal” cache by RMA is 64K8W64B with miss rate 0.0082 and energy dissipation 34.475nJ. By increasing the cache size from 32KB to 64KB, they achieve a significant reduction in miss rate by 30.51% with an increase in energy dissipation by only 0.93%. Thus, the “optimal” cache configuration of 64KB8W64B is reasonable, due to the fact that the reduced miss rate is large enough to overcome the added energy consumed by the cache itself.

C J Janraj, et al. [8] proposed way sharing cache, where two sets share a subset of cache ways apart from having their own cache ways, ways are shared among a pair of sets. The total number of sets in their design is the half of total number of conventional cache have the same degree of associativity.

Their way-sharing cache has 64 pairs of shared sets with 6 ways in each pair, it is denoted as 64×(6, 2)-way sharing DL1 cache. Sharing in their technique enables a flexibility of 2, 3, or 4-way associativity available to each set in the shared pair of sets. Each set of between (0 to 63) of the conventional cache is sharing a set in their way sharing cache with its friend set of between (64 to 127), such that s and p sets own two ways each and share two ways among them.

They run 20 SPEC2000 CPU Benchmarks on modified simplescalar tool and considered the base L1 data cache configuration as 16KB DL1 cache with 4-way associativity and 32B blocks. Hence, the total number of sets in the base L1 data cache is 128. They denoted the base DL1 cache as 128×4-way DL1 cache. Similarly, the base L2 unified cache configuration is referred as 1024×8-way cache with 64B block.

In their results, the 64×(6, 2)-way sharing DL1 cache takes one-and-half times the area of 8KB 4-way DL1 cache and 512×(12, 4)-way sharing unified L2 (UL2) cache takes one-and-half times that of 256KB 8-way L2 cache. Since these are more like approximations, they conservatively consider an additional 10% overhead each for access time, energy and area.

The way-sharing DL1 cache has better per-access energy, area values, and almost equal access time to those of conventional cache, respectively. In the case of UL2 cache with fast-type, the way-sharing mechanism gives better access time and energy with less area. The way sharing mechanism may not be effective in UL2 caches with serial-type as serial-type caches are already optimized for energy consumption.

They consider 512×(12, 4)-way sharing UL2 cache and compare it with 1024×8-way base UL2 cache to know the effectiveness of their way-sharing mechanism when it is applied to unified L2 cache alone. And they consider both serial type and fast-type modes, the way-sharing mechanism is not effective when it is applied to UL2 caches with serial-type and it incurs an average energy overhead of 0.7% (for “gzip” overhead is as the way-sharing mechanism reduces the overall memory energy by 6%. Fast-type L2 caches are generally used in systems when performance is more critical (example, Intel Core family processors). In such systems can apply the way-sharing mechanism in L2 caches also (we observe that it incurs negligible performance penalty).

Jungwoo Park, et al. [9] proposed a cache architecture that can logically increase cache associativity of way-powered-down LLCs. Their proposed scheme is designed to be dynamic in activating an appropriate number of cache ways in order to eliminate the need for static profiling to determine an energy-optimized cache configuration.

They performed experiments using the Sniper simulator and SPEC CPU2000 benchmarks.

They proposed a cache architecture that can be applied to set-associative LLCs. They call this cache architecture “logical–associative cache.”

Their first idea to design the “logical–associative cache” architecture is to activate all tag ways to access them in parallel and not to activate all data ways to reduce their leakage energy consumption. Increasing cache associativity to support parallel access is a very effective solution to increase performance. They compared the execution times, energy consumptions, EDPs, and LLC misses of a two-way 1024-set LLC configuration and a 16-way 128-set LLC configuration. These two cache configurations have the same capacity (256 kbytes). The results shows on average, the 16-way 128-set cache shows 7.4% better performance, 5.4% less energy, and 10.9% less EDP compared with the two-way 1024-set cache.

![Figure 4](image-url) Non filtering parallel logical–associative cache for a four-way cache. (a) and (b) All tag ways are accessed in parallel.
If the capacity is the same, increasing the cache associativity is a good solution for increasing the system performance. Their idea to increase parallelism is shown in Fig. 4, where the tag ways are physically set-associative, whereas the data ways are logically associative within the activated data ways. In this example, cache associativity is four.

They apply logical association to LLCs in which the tag ways are accessed first and then a matching data way is accessed to reduce their dynamic energy consumption. They also proposed the Way-Filtering-based logical-associative LLC architecture to reduce the energy consumption in the tag ways of LLCs, they apply a partial tag matching scheme. It extracts a few bits from the tag bits to early identify a cache miss. A partial tag consists of a few least significant bits from the original tag bits and a few most significant bits from the index bits. Because the cache lines in a cache way are logically divided, the most significant bits (3 bits for eight logical ways) from the index bits are used as part of a partial tag. Its because the number of logical cache sets becomes smaller than that of cache sets when logical cache ways is applied. A partial tag-based way filter is allocated to each cache way, and it is powered down when its corresponding cache way is turned OFF. Experimentally, they find that a 4-bit partial tag and eight logical ways show optimized results.

They evaluated their proposed architecture and observed a 3.4% total system energy and 34% LLC energy savings over the selective-cache-ways scheme with a relatively small overhead on a single-core system. Their proposed scheme shows more energy reduction results on multicore systems with more capacity pressure on the LLC. They observed that the total energy consumption and EDP are reduced by 9.2% and 11.8%, respectively, over the selective-cache-ways scheme on a quad-core system.

Bhargavi R. Upadhyay and Sudarshan TSB [10] surveyed different techniques to find the efficient design space aimed at reducing the design space time and provide good insight to researchers to explore further. Simulation based design exploration leverages software to find the exact cache parameters. Simulators can be classified as a functional simulator, Full system simulator and trace-driven simulator. Functional simulator provides the functional correctness with hit-rate and miss-rate. Functional simulators can be used to trace the memory accesses for the application. They studied several simulators like Simple scalar, SimOS, Simics, Gem5 and trace driven simulators. Trace driven simulators takes a collected memory access pattern for an application as input which gives the output as performance matrix like hit rate. Simulator traces millions of memory reference for the application for the different cache configuration for the application without building the costly hardware. Single pass can take only one configuration, for another configuration we need to run the simulator again. Repeatedly running Simulation process for different configuration of the application can take hours or days.

They mentioned several previously work of reconfigurable cache memory and the hardware units which required for dynamic cache reconfigurations, and also the evolutionary technique which widely used to optimize software and hardware design techniques. Techniques mentioned there are based on offline traces collection and runtime behavior of applications. These approaches used the cache hit ratio, miss ratio, CPI as a performance matrix to evaluate the cache performance.

Safaa S. Omran and Ibrahim A. Amory [11] presented Two Dimensional Reconfigurable Cache memory implemented on FPGA. The design allows reconfiguration in both associativity and size of the cache memory, the memory size can be (64K Byte, 128K Byte, 256K Byte and 512K Byte) and the associativity can be (Direct mapped (DM), 2 way, 4 way and 8 way set associative).

We designed eight sets of cache memory each with size 64K byte, for DM the maximum size is 512K byte and the CPU is dealing with the eight sets as one set with size 512K byte.

For set associative organization the maximum cache size is 512K byte too, hence, the maximum cache memory size for each organization is equal to the already occupied cache memory size, then there is no waste in cache memory size.

The cache design consists of cache size controller unit, cache set controller unit, and cache memory (cache data memory and cache controller which consists of cache tag memory, LRU controller unit, General Mux and finite state machine) as shown in Fig. 5.

**Figure 5. Cache memory design.**

Cache size controller unit responsible for managing the cache size and mapping function, when the processor request an address, this address will be send for the cache size controller unit, the address consists of 32 bits as shown in Fig. 6.

**Figure 6. 32 bits Address**
The required cache size and mapping function are chosen by CPU by sending Size controller signals (4 bits) at run time to the cache size controller unit.

Cache size controller unit produces 6 bits called (I bits) which ANDed with the 6 bits of A [18, 13] produces the index bits which will send to the cache memory to indicate which line is requested to access. At the same time A [18, 13] will be ANDed with another 6 bits called (T bits) to produce the tag bits.

Cache memory size of 512K bytes is divided into 8 sets of cache memory each with size of 64K byte.

- **cache size 64K byte**: with DM the CPU dealing with the first set only with size 64K byte while the other 7 sets is unpowered, with 2 way set associative the CPU dealing with two sets with size 32K byte from each one, with 4 way the CPU dealing with four sets with size 16K byte from each one and with 8 way the CPU dealing with all 8 sets with size 8K byte from each one.

- **cache size 128K byte**: with DM the CPU dealing with two sets as one set with size 128K byte while the other 6 sets is unpowered, with 2 way set associative the CPU dealing with two sets with size 64K byte for each one, with 4 way the CPU dealing with four sets with size 32K byte from each one and with 8 way the CPU dealing with all 8 sets with size 16K byte from each one.

- **cache size 256K byte**: with DM the CPU dealing with four sets as one set with size 256K byte while the other 4 sets is unpowered, with 2 way set associative the CPU dealing with four sets as two set with size 128K byte for each one, with 4 way the CPU dealing with four sets with size 64K byte for each one and with 8 way the CPU dealing with all 8 sets with size 32K byte from each one.

- **cache size 512K byte**: with DM the CPU dealing with all 8 sets as one set with size 512K byte, with 2 way set associative the CPU dealing with 8 sets as two set with size 256K byte for each one, with 4 way the CPU dealing with four sets with size 128K byte for each one and with 8 way the CPU dealing with all 8 sets with size 64K byte for each one.

The dealing of CPU with several sets of cache as one set is controlled by Cache way controller unit, depending on the selected cache size and associativity and on the location of requested line, each set covered 64K byte (4096 Line each with size 16 byte).

Fig. 7 shows the all 8 sets of cache memory each with size 64KB. While a 256KB cache size selected with Direct Mapped organization. The CPU now dealing with the first 4 sets as one set of cache memory with size 256KB. While another 4 sets with red color unaccessed.

Fig. 8 shows a 256KB cache size selected with two way set associative. The CPU now dealing with the first 2 sets (Set1 and Set2) with blue color as Way0 with size 128KB and with Set3 and Set4 with green color as Way1. While another 4 sets with red color unaccessed.

In case of Cache full size 512KB and 8 Way set associative. Each set individually representing way of 8 ways of cache memory.

Way Controller Unit is controlling the dealing of CPU with several sets as one cache memory set.

General Mux responsible for connecting the input and output data buses to and from cache sets relying on the signal (Dwith) which sent from FSM. LRU controller Unit indicates which way least recently used in case of set associative is selected.

The two dimensional reconfigurable cache memory implemented using FPGA (Field-Programmable Gate Array).

### III. RESULTS

A complete design of a 32-bit MIPS (Microprocessor without Interlocked Pipeline Stages) is used to test the
reconfigurable cache memory by execute several test programs.

A direct mapped cache less time access because it accesses only one tag and data array per access, while in set associative cache memory the cache accesses many tag and data arrays per access.

For some applications a DM cache memory exhibits a very poor hit rate and this causes poor performance. Adding set associativity increases the hit rate, but for many applications, the additional associativity is unnecessary and thus results in wasted energy and longer access time.

In this paper a model of a maximum cache size up to 512KB for any mapping function was designed. A 512KB cache size for direct mapped, 2-way, 4-way or 8-way can be selected and the design is programmed using VHDL and implemented on FPGA.

The technique were used in this design is different from other papers were they need more amount of cache size from the used size. For example in smart cache design they need 8MB cache size to implement a 2MB cache of reconfigurable 4-way, 2-way or Direct Mapped cache memory.

IV. CONCLUSIONS

From the comprehensive studies for several papers of reconfigurable cache memory. It is clear that the reconfigurable cache memory is important to improve the cache performance and reduces the energy consumption.

The performance of the cache memory is largely determined by the specific application. Different applications achieve better energy-performance with different configurations of the cache memory hierarchy.

The direct mapped have better access time and energy saving feature but it have higher miss rate compare with the set associative mapping which have longer access time and more energy consumption.

REFERENCES

Design SHA-2 MIPS Processor Using FPGA

Safaa S. Omran 
Computer Engineering Techniques College of 
Electrical and Electronic Techniques Baghdad, 
Iraq
Omran_safaa@ymail.com

Laith F. Jumma 
Computer Engineering Techniques College of 
Electrical and Electronic Techniques Baghdad, 
Iraq
Laith1993@gmail.com

DOI: 10.24086/cocos17.02

Abstract— According to the wide developments in the area of communications, there is a demand for secure system for data transmissions. Hence, a new algorithm and security standards are developed. One of these algorithms and standards are the Hash function. In this paper, a Hash system SHA-2 MIPS (Microprocessor without Interlocked Pipelines) Processor (single cycle) is designed using Xilinx Spartan-3AN interfaced with keyboard and Video Graphics Array (VGA) display. The implementation of the MIPS processor by choosing a certain number of instructions that is necessary to invoke the SHA-384 and SHA-512 algorithm. A keyboard is interfaced with the Xilinx Spartan-3AN kit, to enable the user to enter the data and the result is shown on a VGA Display.

Keywords—VHDL; SHA-2; MIPS Processor

I. INTRODUCTION

A variation on the message authentication code is the one-way hash function. A hash function accepts a variable-size message \( M \) as input and produces a fixed-size output, referred to as a hash code \( H(M) \). Hash functions are used in conjunction with symmetric ciphers for digital signatures. In addition, hash functions are used for message authentication [1].

VHDL (Very High Speed Integrated Circuit Hardware Description Language) is a hardware description language. It describes the behaviour of an electronic circuit or system, from which the physical circuit or system can then be attained[2].

One of the earliest hardware designs of hash function is reported by selimis in [3]. The authors in [4] propose a processor for both SHA-1 and MD5 algorithms, and implemented on an Altera Apex 20k. While in [5] a high-performance SHA-1 design in presented and implemented on a Xilinx Vertex-E FPGA. The authors in [6] implement a SHA-1, HAS-160 and MD5 in one chip. In [7] a processor is designed to support the algorithm of SHA-1 and SHA-256 hashing. However, in this research SHA-384 and SHA-512 hash MIPS processor with keyboard and VGA display is designed and implemented using Xilinx Spartan-3AN.

II. SHA-2 ALGORITHMS

The SHA-2 namely SHA-384, and SHA-512 have several commonalities. SHA-2 algorithms are one-way hash functions that process a message to produce a message digest. This paper was implemented SHA-384 and SHA-512 hash algorithms. Each algorithm can be classified into two stages.

The first stage is the Pre-processing stage and the second is Hash Computation.

A. Pre-processing

SHA-2 input block size various depends on what algorithm is used. In this stage the message is padded into block size called chunk. The input blocks size of SHA-384 and SHA-512 is equal to 1024-bits divided into 16 words \( W[0-15] \) of 64-bits. Then extending the 16 words \( w[0-15] \) depending on a certain algorithm. Table I shows features of the two hash functions.

B. Hash Computation

Hash Computation various depending on the algorithm used if it is SHA-384 or SHA-512.

- SHA-512 Computation

The message digest is 8 hash variables each of 64 bits are used. It take 80 rounds to completed SHA-384 and SHA-512 calculation. SHA-512 algorithm is done as follows:

In the first step hash variables shown in table II and are initialized.

In the second step message words \( W[0-15] \) extended into 80 words \( W[16-79] \)

\[
S0 = (W[t-15] >>> 1) \oplus (W[t-15] >>> 8) \oplus (W[t-15] >>> 7)
\]

\[
S1 = (W[t-2] >>> 19) \oplus (W[t-2] >>> 61) \oplus (W[t-2] >>> 6) \hspace{1cm} (1)
\]

\[
W[t] = W[t-16] + S0 + W[t-7] + S1
\]

Where >>> is right rotate and >> is right shift
In the third step 8 variable (A to H) is added which are equal to (H0 to H7)

The fourth step is the main loop where (A to H) will be calculated in 80 Round as follow:

\[
\text{TEMP1} = H + S1 + CH + K[t] + W[t] \\
\text{TEMP2} = S0 + MAJ \\
H = G \\
G = F \\
F = E \\
E = D + \text{TEMP1} \\
D = C \\
C = B \\
B = A \\
A = \text{TEMP1} + \text{TEMP2}
\]

where \(K[t]\) is round constants and \((S0,S1,CH,MAJ)\)

\[
\begin{align*}
V0 &= (A >>> 28) \oplus (A >>> 34) \oplus (A >>> 39) \\
V1 &= (E >>> 14) \oplus (E >>> 18) \oplus (E >>> 41) \\
CH &= (E \& F) \oplus \neg (E \& G) \\
MAJ &= (A \& B) \oplus (A \& C) \oplus (B \& C)
\end{align*}
\]

The final step is adding (A to H) with (H0 to H7) which produce the massage digest of 512-bit.

\[
\begin{align*}
H0 &= H0 + A \\
H1 &= H1 + B \\
H2 &= H2 + C \\
H3 &= H3 + D \\
H4 &= H4 + E \\
H5 &= H5 + F \\
H6 &= H6 + G \\
H7 &= H7 + H
\end{align*}
\]

- **SHA-384 Computation**

SHA-384 and SHA-512 are identical algorithms except that:

The message digest in 384-bit is constructed by omitting \((H6-H7)\).

The initial hash values for SHA-384 are different from that of SHA-512.

\[
\begin{array}{|c|c|c|c|}
\hline
\text{TABLE III. INITIALIZED SHA-384 VARIABLE} \\
\hline
H0 & H1 & H2 & H3 \\
\hline
CBBB9D5D & 629A292A & 9159015A & 152FEC9D8 \\
C1059ED8 & 367CD807 & 3070DD17 & 70E5939 \\
H4 & H5 & H6 & H7 \\
67332667 & 8EB4A487 & DB0C2E0D & 47B5481D \\
FFC00B31 & 68581511 & 64F98FA7 & BEFA4FA4 \\
\hline
\end{array}
\]

Fig. 1 shows a block diagram for SHA-2 computation.

Fig. 1 shows a block diagram for SHA-2 computation.

![SHA-2 Computation](image)

**III. INSTRUCTION SET ARCHITECTURE SIZE**

**MIPS** processor uses 32-bit for each instructions. MIPS defining three instruction formats: R-type, I-type, and J-type. **R-type** instructions have three registers. **I-type** instructions have two registers and a 16-bit immediate value. **J-type** instructions have one register and a 26-bit immediate.

- **R-type Instructions**

R-type instructions have three registers as operands: two as sources and one as a destination.

It has six fields: funct(function) ,op(opcode), rs(source register), rt(target register), rd(destination register) and shamt(shift operations). Each field is five or six bits, as indicated in fig.2a.

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>rd</th>
<th>shamt</th>
<th>funct</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-bit</td>
<td>5-bit</td>
<td>5-bit</td>
<td>5-bit</td>
<td>6-bit</td>
<td></td>
</tr>
</tbody>
</table>

**I-Type Instructions**

I-type instructions have two register operands and one immediate operand. It has four fields: imm ,op, rs and rt. The first three fields op, rs and rt, are like those of R-type instructions. The imm field holds the 16-bit immediate, as indicated in fig.2b.

<table>
<thead>
<tr>
<th>Op</th>
<th>rs</th>
<th>rt</th>
<th>imm</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-bit</td>
<td>5-bit</td>
<td>5-bit</td>
<td>16-bit</td>
</tr>
</tbody>
</table>

**J-type Instructions**

This format is used only with jump instructions. This instruction format uses a single 26-bit address operand, addr. **J-type** instructions begin with a 6-bit immediate.

The remaining bits are used to specify an address addr, as indicated in fig.2c.

<table>
<thead>
<tr>
<th>op</th>
<th>addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-bit</td>
<td>26-bit</td>
</tr>
</tbody>
</table>

**IV. PROCESSOR DESIGN**

The single-cycle microarchitecture executes an entire instruction in one cycle. It is easy to explain and has a simple
control unit. Because it completes the operation in one cycle it does not require any nonarchitectural state. However, the cycle time is limited by the slowest instruction [8-9].

In this research few instructions were implemented in the design only the instructions that requires to invoke the algorithm of SHA-384 and SHA-512 were implemented using VHDL in Xilinx ISE software environment.

Since SHA-384 and SHA-512 hash variable is 64-bit so in this paper a MIPS single-cycle processor of 64-bit is designed for SHA-384 and SHA-512.

The simple design of a 64-bit, single cycle MIPS processor consists of two parts:

- 64-bit Datapath
- Control unit.

A. 64-bit Datapath

A 64-bit single cycle MIPS processor requires a 64-bit datapath. It contains element such as registers, memories, ALUs, sign, extenders and multiplexers.

A description for each datapath is shown below:

a. Program counter (PC): is a register represents the address of instruction to execute which has 32-bit size.

b. Instruction memory: store instructions used to execute hash function and consist of a 64-bit data as its output.

c. Register file: consist of 32 registers, each has 64-bit in size. It has two read port and one write port.

d. Data memory: has one input write port (WR) and two output read ports (RD). The input is written in memory which specified by the address (A) if (WE) signal is 1 at the raising edge of (clk) signal, each memory location is 64-bit size.

e. Sign extension simply copies the most significant bit of a 16-bit input size.

f. ALUs is used in order to execute the arithmetic and logical instructions. ALUs take alucontrol(2:0) as input and generate corresponding function. Note that there are modification in some instruction.

B. Control unit

The control unit receives from the instruction memory the current instruction funct(5:0) and Opcode(31-26) of the datapath which tell it what to do to execute the instruction.

Fig.3 shows the complete design of the MIPS processor of 64-bit and table IV shows all instructions required to invoke the SHA-384 and SHA-512 algorithms.

<table>
<thead>
<tr>
<th>Instruction</th>
<th>SHA-384</th>
<th>SHA-512</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMP</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>LOAD</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>STORE</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ADDI</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>BEQ</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XOR</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>AND</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NOT</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>OR</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ADD</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 28</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 34</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 39</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 14</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 18</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 41</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 1</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 8</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 19</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RR 61</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SR 7</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SR 6</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

TABLE IV. MIPS Instruction and Where It Used

Fig.3 Block diagram of MIPS Processor
V. KEYBOARD & VGA DISPLAY INTERFACE

A keyboard consists of a matrix of keys and an embedded microcontroller that monitors (i.e., scans) the activities of the keys and sends scan code accordingly [10]. For example, when we press and release the N key, the keyboard first transmits its make code (31) and then the break code (F0 31).

The information is transmitted as an 11-bit “packet” that contains a start bit, 8 data bits, an odd parity bit, and a stop bit, as shown in Fig 4.

The FPGA application have eight colour corresponding to VGA port with a three-bit interface as shown in table VI.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>Black</td>
</tr>
<tr>
<td>0000</td>
<td>0000</td>
<td>1111</td>
<td>Blue</td>
</tr>
<tr>
<td>0000</td>
<td>1111</td>
<td>0000</td>
<td>Green</td>
</tr>
<tr>
<td>0000</td>
<td>1111</td>
<td>1111</td>
<td>Cyan</td>
</tr>
<tr>
<td>1111</td>
<td>0000</td>
<td>0000</td>
<td>Red</td>
</tr>
<tr>
<td>1111</td>
<td>0000</td>
<td>1111</td>
<td>Magenta</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>0000</td>
<td>Yellow</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>1111</td>
<td>White</td>
</tr>
</tbody>
</table>

In this research take White Resulting black to show the character and screen background. The patterns of the tiles is 8-column-by-16-row for each character since the resolution screen is 640-by-480, 80 tiles can be fitted into a horizontal line and 30 tiles can be fitted into a vertical line. Fig 5 shows the ROM content of the letter “F”.

VI. RESULTS

The word “abc” was entered from the keyboard and the result of SHA-384 and SHA-512 is displayed on VGA display as shown in Fig 6. The test simulation for the word “abc” is shown in Fig. 7 and Fig. 8.
A hash SHA-384 and SHA-512 was implemented using FPGA Spartan-3an. A MIPS processor was designed using VHDL Xilinx ISE software language with only instructions that Hash need. This study is a starting point for future studies and can be extended to invoke the algorithm for SHA-384 and SHA-512 by using a superscalar MIPS processor.

Fig 6-a the massage digest of SHA-512 and time require.

Fig 6-b the massage digest of SHA-384 and time require.

REFERENCES


A comparative analysis between low and high level HoneyPots

Rebin B. Khoshnaw
College of Science
Salahaddin University Hawler
Erbil, Iraq
Rebin.saleh@su.edu.krd
DOI: 10.24086/cocos17.03

Abstract— The concern of information security and data protection is growing and getting more critical day by day within organizations and companies. This has led developers and researchers to find advanced ways of defense against attacks on networks. One of these ways is using Honeypots. Honeypot is an information security resource used to protect network resources in the way of diverting attackers from their real targets. At the same time, it is used as a tool intended to be attacked and compromised to collect information about attacks that organizations might face and use the collected data to develop methods for protection against these attacks. Honeypots generally come in many forms and shapes, and they are classified according to the level of interaction with attackers. Low interaction Honeypots are easy to maintain and deploy with few risks. High interaction Honeypots are more advanced in terms of maintenance and deployment and more risky but they will gather more extensive and accurate information than low interactive Honeypots. The aim of this paper is to provide a review on Honeypots. It also analyses Honeypots under three (3) main categories: Implementation, effectiveness and limitation in the security field.

Keywords: Honeypot, Security, low interaction, high interaction, implementation, performance and limitations

I. INTRODUCTION

As world population increases each day, the usage of internet is increasing too. Simultaneously, number of cyber criminals are increasing and causing enterprises and organizations huge financial losses by taking advantage of existence vulnerabilities. The privacy and security of each user has become more important concern. There are many tools and technologies that provide security such as firewall, intrusion detection and prevention system. But, usually these tools and technologies give gigabytes of information and in turn it’s needed to dig in to it to get the required useful information.

In military actions, it is critical to know the behavior of enemies, how they attack, what tools they use, which path they take and what they are targeting. This information is used to fix vulnerabilities. To collect such information without the awareness of the attacker, a tool is used called Honeypot.

There are various definitions of Honeypot given over the years by different researchers and developers in this area which causes misconception and confusions in the definition of the term. Some think that it is a weapon against hackers, while some others say it’s a tool used for deception. On the other hand, some researchers in this area consider it as a tool for intrusion detection. Spritzner defined Honeypot as “a security resource whose value lies in being probed, attacked or compromised” [1]. According to Spritzer’s definition, it could be said that Honeypot is used as a system to be attacked and compromised so that the information about the attacker is gather in this way. No matter if it’s a router or a production system, as far as its attacker by the hacker.

Since late 80’s, firewalls have been used as an initial design to prevent or slow down hacker’s attacks and threats [2]. As a new security layer beside firewalls, intrusion detection system (IDS) and intrusion prevention system (IPS) technologies, Honeypots were invented. David Watson and Lance Spitzner in their publications agree on that the early publications about Honeypots were by Clifford Stoll and the white paper by Bill Cheswick in 1990/1991 [1, 3, 4]. Furthermore, Lance Spitzner in his [1] mentioned the history of Honeypots in details. In 1997, one of the first Honeypot solutions in the name of Fred Cohens Deception toolkit was released. In 1998, first commercial Honeypot called CyberCop was sold to the public. In the same year, Back Officer Honeypot which is a free product was released. Honeypot Project was formed in 1999 [5]. In 2000/2001, organization started to use Honeypots for researching and detecting new threats[1, 6, 7].

In general, attacks are divided into four categories which are interception, interruption, modification and fabrication. Security is under risk due to these types of attacks. Each of them is targeting different aspects of security which are availability, confidentiality and integrity of the data. Availability means providing information 24/7 to authorized people any time they want to access them. Confidentiality is about not allowing users to access critical information if they do not have permission while Integrity means making sure that the data is not being changed by preventing attackers from doing so.

The significant ideas behind this paper are to make a comprehensive and analytical review on the low and high interaction Honeypots.

As a matter of fact, the community doing research around Honeypots focuses on revision of a single aspect of Honeypot...
whether it is Implementation, effectiveness or limitation. Authors believe that there are no critical review done which contain all the above mentioned aspects of Honeypot, hence makes a gap in this research area. Therefore, the scientific contribution of this paper will help filling the gap by critically reviewing Honeypots and give comprehensive and analytical comparison of Honeypot types.

For that, this paper presented in the following structure. In the previous section, a literature review has been presented regarding Honeypots. In the next section, the advantages and disadvantages of Honeypots are presented. After that Honeypot architecture will be followed. This is followed by analytical comparison between types of Honeypot. The paper ends with a conclusions section.

II. ADVANTAGES AND DISADVANTAGES OF HONEYPOTS

Honeypot has powerful strengths due to the simple concept it has. Below are some advantages described by Spitzner and Niels Provos [1, 8, 9]:

1- Small data set: Honeypots give precise information about the attacker in a quick and understandable way. This leads to immediate analysis and reaction toward attackers.
2- Encryption: regardless of whether the attack is encrypted or not, Honeypot will detect it as soon as there is an interaction with it.
3- Minimal resource: Honeypot can do its work even with a simple computer. This makes it require minimal resource.
4- IPv6 and IPv4: it works in both IPv6 and IPv4 environment. Even if an attacker uses IPv6, it will be detected.
5- Highly flexible: Honeypots can be used in different sized networks regardless how big the network is.
6- Reduced false positives and detecting false negatives.

Honeypots have several disadvantages beside the aforementioned advantages like all other technologies [1, 8, 10]

1- Limitation in the view: Honeypots can gather information regarding threats and attacks interacting with them. They don’t have the ability to detect threats outside the Honeypot network.
2- Risk: there is a probability that the attacker use the Honeypot system to attack other organizations and networks without Honeypots.

Spitzner also mentioned another disadvantage which is fingerprinting. An attacker has some behaviors put in mind regarding systems, whenever these behaviors are detected, then the attacker will identify the Honeypot based on these characteristics.

III. USAGES OF HONEYPOTS

Honeypots are used in various ways for different purposes. Authors (Roger A Grimes, thehoneypotproject and David Watson) agree on some general usages stated below [3, 5, 11]

1- Attack prevention
2- Attack detection
3- Attack responding
4- Research purposes

Grime in [11] outlined the reasons of using Honeypots in the following points:

1- Honeypots give less false positive. What is meant by false positive? This is when a security tool indicates a non-malicious activity as a malicious.
2- Honeypots are used to detect threats earlier since they give lower rate of false positive
3- Honeypots do not differentiate between detecting new unknown threats and known attacks. They are capable of gathering info about the attack even if it is unknown.
4- By using Honeypots, organizations and researchers will know who they are dealing with and know their enemy in the way that reveals what techniques they are using and the way they attack.
5- Usually Honeypots are configured as a security layer after firewalls, IDS and IPS, so any threat made through the firewall, IDS and IPS will be detected by Honeypots.
6- Honeypots are being used in research area to find vulnerabilities of systems and networks.

IV. HONEYPOT ARCHITECTURE

Honeypots are real systems configured with the high interaction capability to be attacked by hackers. To successfully deploy a Honeypot architecture, three important elements are required which are data control, data capture and data collection [5, 12-14]. The general Honeypot architecture is shown in figure 1.
Data control: it gives space to the attacker to perform activities required for compromising, the more freedom is given to the attacker to operate, and the more data is being collected about the attacker. However, more space allowed, the probability of putting the system in to risk will increase and the attacker may use the system to attack other organizations.

Data capture: is the process of monitoring all the activities performed by attackers and then analyze them to learn more about the way and technique used by the hacker.

Data collection: when an organization has many Honeypot systems spread around the world, a data collection technique is required to collect the information from all Honeypots centrally.

V. LOW AND HIGH LEVEL HONEYPOTS

As mentioned before, there are two types of Honeypots. Basically, they are low interaction and high interaction Honeypots.

In low interaction Honeypot, the honeypot is designed in a way that attacker attack only a hard disk provided by the honeypot owner through the operating system without putting other local resources in danger as it can be seen from figure 2. Low interaction Honeypots require less resources and they are less complex hence they need less code and they require much less response time.[1, 7]

On the other hand, high interaction Honeypots are designed in such way that the intruder attack most of the resources provided by the Honeypot owner so that the intruder spend as much time as possible on the network so that enough information is collected from the attacker. As it can be seen from figure 2, the intruder is permitted to access Hard disk as well as other local resources to waste the time. In general, high interaction Honeypots provide more security by being difficult to detect but they are difficult to be configured and maintained. High interaction Honeypots are more complex therefore they require more coding.
Since a part of the technologies which are implemented, effectiveness/performance and limitation [15-18].

1- Implementation
High interaction Honeypots have a real operating system and machine dedicated to them and allow the attacker to have full access to the machine. High interaction between the attacker and the Honeypot will lead to gathering extensive amounts of information about the thread.

On the other hand, low interaction Honeypots are simpler, easier to deploy, and easier to maintain since a part of the system or some specific service such as mail service is available for the hacker to attack it.

2- Effectiveness/Performance
Both low and high interactions Honeypots have some flaws in their performance as do other security tools and technologies in spite of having discussed advantages.

a) Turning against administrator
Since high interaction Honeypots are involved completely with the attacker, there is a possibility that the attacker uses the Honeypot to attack other systems and act against the administrator while low interaction type is safer in this point since the system is partially available for the attacker.

b) Zero day exploits
Zero day attacks are more dangerous than normal attacks since they leave no time to respond [19]. Because of their simplicity in the algorithm they use, low interaction Honeypots are not well suited to capture zero day exploits. To solve this problem, high interactions are used due to extensive information gathered by them using complex algorithms.

c) Failure effects
The writers believe that the failure of high interaction Honeypots is much more than the low interaction type. Failure of low interaction Honeypots will not cause severe damages since they are an illusion of the machine. While high interaction Honeypots are real systems, if they fail, the attacker would use them to send active and passive attacks to other systems and organizations.

3- Limitations
Honeypots can only gather information about threads that interact with them. They are unable to detect threads outside the Honey net. This is a limitation shared by both the low and high interactions Honeypots [16].

It is believed that due to their low interactions, enough information about the attacker may not be collected and hence may not help the organization to track the attacker.

VI. CONCLUSION
Honeypots are a new technology which is emerging into networking and internet world. Due to their significant advantages, they can be applied to different environments with different sized network either it is large or small. A well configured Honeypot will get valuable information on attacks and the attacker. Beside their ability of reducing false positives, they could be deployed in different sized network because of their flexibility and scalability. For thread detection environment, low interaction Honeypots is sufficient and will do the work. But if extensive information is required, high interaction Honeypots is the solution.

This paper showed that both types of Honeypots are effectively used against attacks, but each has its own drawbacks. To overcome these Achilles heel, the author believes that Honeypots should be configured and put in a way after firewalls, Intrusion detection and Intrusion prevention systems so that if a threat was successful to pass over them then it will be caught by Honeypot. So the system will have an extra layer of security against turning the Honeypot against administrator.

Author believes that Implementation, performance and limitations of Honeypots must be considered for developers when adapting a Honeypot for monitoring and auditing traffic over the network.

The comprehensive and analytical review and comparison between Honeypot types in this paper opens the door for
researchers as a future works to implement or improving low and high interaction Honeypots.

REFERENCES


Comparative Study for Color Edge Detection Using Vector Value, YCbCr Color Space and Least Square Numerical Method

Sarah Behnam Aziz  
College of Sciences,  
Computer Science & IT department  
Salahaddin University  
Erbil, IRAQ-KRG  
sarah.aziz@su.edu.krd

Dalya Abdullah Anwer  
College of Sciences,  
Computer Science & IT department  
Salahaddin University  
Erbil, IRAQ-KRG  
dalya.anwar@su.edu.krd

Mardin A. Anwer  
College of Engineering  
Software and Informatics Department  
Salahaddin University  
Erbil, IRAQ-KRG  
mardin.anwer@su.edu.krd

DOI: 10.24086/cocos17.04

Abstract— Edge detection plays an important role in image processing, pattern recognition and computer vision applications. Most of edge detection schemes are based on finding maximum in the first derivative of the image function or zero crossings in the second derivative of the image function. Various methods of edge detection for color images, including techniques extended from monochrome edge detection as well as vector space methods are presented. This research presents a comparative study on different methods of edge detection of color images. The methods are based on vector space, color space and numerical methods. Seven different colored images are test in this research. Performance is analyzed depending on Mean Square Error (MSE). The experimental results show that applying vector value (Jacobian method) will create a thick and disconnected edge with all operators Sobel, Prewitt and Log. While the least square method produce edges that are much thicker but continuous. The best performance was found when using YCbCr luminance (Y) and chrominance (Cb and Cr) method, the edges are sharpened, continuous, and not thickness. They are similar with Sobel and Prewitt operators nonetheless with some missing edges while it is better with Log operator.

Keywords: Edge detection; least square numerical method; Sobel operator; Prewitt operator; log operator; Jacobian eigenvalue.

I. INTRODUCTION

Edge detection is the first manipulated process toward recognizing objects in a complex scene of image understanding system [1]. We can define the edge as a boundary between an object and the background. Lots of approaches have be discover to obtain edge detection [2]. Yet most of these methods are categorized into two types. First derivative-based edge detection operator to detect image edges by computing the image gradient values, such as Roberts operator, Sobel operator, Prewitt operator; and the second derivative-based edge detection operator, by seeking in the second derivative zero-crossing to edge detection, such as LOG operator, Canny operator [3,4]. Gradient is a measure of the function changes and it is the first order derivative of the image corresponds to two-dimensional function.

Image can be defined as a series of derivative of image intensity of sampling points group. Gradient is a type of two-dimensional equivalent of the first derivative. Therefore, it can be defined as a vector [5]. Edges mostly divide into step shape and roof shape. Equation number 1 represent digital image’s first-order partial derivatives such as water droplet image which has step edge.

\[
\begin{align*}
    f_x &= f(x + 1, y) - f(x, y) \\
    f_y &= f(x, y + 1) - f(x, y)
\end{align*}
\]

The following approximate formula is used to simplify the calculation of gradient:

\[
grad(x, y) = |f_x| + |f_y|
\]

Across operator detects the gradient which cross along with the image coordinate axis 45° and 135°.

\[
grad(x, y) = |f_x| + |f_y|
\]

Other common operators include Prewitt operator, Sobel operator, and Laplace operator [6].

A. Vector Value Method

The vector-valued technique is applied on the color images and isolate individual component of RGB. Whereas in grayscale images a discontinuity in the grayscale function is term as an edge. The term “color edge” is not evidently defined for color images. There are plenty of different definitions are proposed for color edges. G.S Robison in 1976 said that the intensity image contains an edge only when the edge exists precisely in the color image [7]. In addition, the other definition of G.S Robison of color edge detection is that, if at
least one of the color components contains an edge only then edge exist in color image. Yet, when edges are merged in edge detection then the color components may cause some problems due to localization inaccuracies of edges in the individual color channels. The third definition of G.S Robison to detect the color edges it is based on the sum of absolute values of the gradients for the three color components (RGB).

The results of the color edge detection by the previously named definitions depend heavily on the used color spaces. A color image represents in the terms of vector-valued function; a discontinuity of chromatic information can also be defined in a vector-valued way.

Henriques in 2010 suggested a method of edge detection that depends on vector-valued techniques, in which the direct formulas for the Jacobian eigenvalues were used, so this function is vectorized and yields good results without sacrificing performance [8]. The main steps of Jacobian method can be explained briefly as following:

1. Determine the standard edge detection operator that will to be applied.
2. Compute the x-direction derivative (rx, gx, and bx) for the three color component (RGB) separately.
3. Compute the y-direction derivative (ry, gy, and by) for the three color component (RGB) separately.
4. Compute the Jacobian matrix for the x-direction derivatives, y-direction derivatives and their combination.
   \[ J_x = r_x^2 + g_x^2 + b_x^2 \]
   \[ J_y = r_y^2 + g_y^2 + b_y^2 \]
   \[ J_{xy} = r_x r_y + g_x g_y + b_x b_y \]
5. Compute first (greatest) eigenvalue (e1) of 2x2 matrix J.\(^\ast\)J.
   \[ D = \sqrt{\text{abs}(J_{x}^2 - 2J_{xy}J_{y} + J_{y}^2 + 4J_{xy}^2)} \]
6. Find the edge magnitude.
   \[ \text{edge magnitude} = \sqrt{e_1} \]

B. YCbCr Color Space Methods

YCbCr color space uses for component digital video. It scales and offset version of the YUV color space. YUV space corresponds to the RGB color cube the YCbCr color space. It is crucial to convert the RGB color image to YCbCr color using equations 10-12 when applying edge detection in YCbCr color space. Then applying the required edge operator on the result of equation 11 (the luminance Part (Y)) and reconverted it again to RGB color space.

It is important to convert the RGB color image to YCbCr color using equations 10-12 when applying edge detection in YCbCr color space. Then applying the required edge operator on the result of equation 11 (the luminance Part (Y)) and reconverted it again to RGB color space.

C. Least Square Numerical Method

Al-Nifaay in 2005 suggested a method of edge detection that depends on the algorithm of least square curve fitting. They took a sliding mask (like 3x3) and took some steps to detection an edge point in this mask if it's found [11]. In the first step, they rearrange the pixels of this mask in a pair \([x, y(x)]\), where \(x\) represents the location (index) of the color levels values \(y(x)\). \([x=1, 2, 3... n]\), \(n\) is the total number of pixels in the mask.

The relation then modify in the form of a straight-line relation given in the equation.

\[ Y(x) = a + b \times \] (16)

Where \(a\), \(b\) are constant can be obtained in the following:

- Compute the summation
  \[ \sum_{x=1}^{n} \sum_{y=1}^{n} x y(x) \]
  \[ \sum_{x=1}^{n} x^2, \sum_{x=1}^{n} x, y(x) \]
  (17)
- From the least square approximation method, we calculate \(a\) and \(b\):
  \[ b = \frac{n \sum_{x=1}^{n} x y(x) - \sum_{x=1}^{n} y(x) \sum_{x=1}^{n} x}{n \sum_{x=1}^{n} x^2 - (\sum_{x=1}^{n} x)^2} \]
  \[ a = \frac{\sum_{x=1}^{n} y(x) - b \sum_{x=1}^{n} x}{n} \]
(19)

The least square curve fitting method can be obtained from equation (19) depends on the values of \(a\) and \(b\) [11].

The paper is organized as follows: An introduction of edge detection is given in Section 1. Previous related works are presented in Section 2. Section 3, introduce the experiments and results of the comparing the three methods: vector Value (Jacobian), YCbCr Color Space and Least Square Numerical Method.
II. RELATED WORKS

It is noteworthy that currently there is no research that undertaken vector value, YCbCr color space and least square numerical methods in comparing color edge detection. However, most of researches are done on comparing the traditional methods on edge detection. Therefore, in our related work we will refer to some papers that focused on edge detection in general. Amer in 2005 detected the edge for many real color image that represented the type of digital image by using a new operator in least square approximation method which is a type of the numerical method [11].

Bhadauria in 2008 presented a brief study of the fundamental concepts of the edge detection operation, theories behind different edge detectors and compares different image edge detection algorithms including Roberts, Sobel, Prewitt, and Canny with MATLAB tool in his paper [12].

While (Hassan, 2013) presented an edge detection method applicable to grey level images based on Approximation Theory. He compared the performance of his proposed method with other methods such as Sobel and Prewitt edge detector by using various tested images. The experimental results in the research reveal that the proposed method exhibits better performance and may efficiently for the detection of edges in image [13].

Ahmed in 2013 proposed a new algorithm for detection the edge in biomedical images depends on least square approximation method, which considered one of the types of the numerical methods. They focused on edge detection task in biomedical images, which is a key problem. They showed how the proposed method cans detection on the edge in images with high efficiency compare with standard methods [14].

Rupinder Singh and Jarnail Singh in 2011 proposed algorithm that designed for integrating edges and regions. The edge map of image is obtained by using canny edge operator [15]. In the same year, Nagabhushana Rao illustrated the comparative analysis of various image edge detection techniques on finger print images [16]. While in 2010 Jagadish H. Pajar, proposed a novel algorithm for medical image segmentation according to vigorous smoothening by recognizing the type of noise and edge detection ideology which seems to be a boom in medical image diagnosis [17].

In 2009, Andres described a new line segment detection and extraction algorithm for computer vision, image segmentation, and shape recognition applications [18].

Maik and Kumar (2016) applied Canny's edge detection technique on color and grey scale images. They observed that the Canny’s edge detection algorithm performs better than all other methods under almost all scenarios it gives better result in gray scale images and color [19].

III. RESULT AND DISCUSSION

In this paper, various color edge detection methods namely vector Value, YCbCr color space and least square numerical method are applied on seven different colored shapes. For implementation, Matlab R2013 is used on a computer that has Intel(R) Pentium (R) CPU with 4GB RAM. The results of these methods are shown in figure 2-8 respectively. In the other hand the algorithm used in this paper are shown below.

Start
For i=1 to 7 do the following
Begin
Select colored image
X= detect edge using Least Square Method
Y1= detect edge using YCbCr Method using Sobel
Y2= detect edge using YCbCr Method using Prewitt
Y3= detect edge using YCbCr Method using log operator
Z1= detect edge using Jacobian Method using Sobel
Z2= detect edge using Jacobian Method using Prewitt
Z3= detect edge using Jacobian Method using log operator
Evaluate MSE for X, Y1, Y2, Y3, Z1, Z2, Z3
End
End

Figure 2. The algorithm used in implementing the program

Figure 3. Edge detection results of image 1, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.
Figure 4. Edge detection results of image 2, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.

Figure 5. Edge detection results of image 3, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.

Figure 6. Edge detection results of image 4, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.

Figure 7. Edge detection results of image 5, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.
Figure 8. Edge detection results of image 6, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.

Figure 9. Edge detection results of image 7, a: original image, b: least square, c: YCbCr Sobel, d: YCbCr Prewitt, e: YCbCr log, f: Jacobian Sobel, g: Jacobian Prewitt, h: Jacobian Log.

Table 1 represent the result of MSE for images 1, 2, 3, 4, 5, 6 and 7. MSE is The Mean Square Error (MSE). It is used to compare image edge detection quality. The MSE value gives the average difference of the pixels throughout the original image with edge detected image. The higher MSE indicates a greater difference between the input image and resultant image [20].

<table>
<thead>
<tr>
<th>Image</th>
<th>Numerical Method</th>
<th>YCbCr Method</th>
<th>Jacobian Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Least Square</td>
<td>Sobel</td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td>Sobel</td>
<td>Prewitt</td>
<td>Log</td>
</tr>
<tr>
<td>1</td>
<td>0.2405</td>
<td>0.2769</td>
<td>0.2689</td>
</tr>
<tr>
<td>2</td>
<td>0.2156</td>
<td>0.0974</td>
<td>0.2122</td>
</tr>
<tr>
<td>3</td>
<td>0.6244</td>
<td>0.3487</td>
<td>0.3392</td>
</tr>
<tr>
<td>4</td>
<td>0.4170</td>
<td>0.4090</td>
<td>0.4089</td>
</tr>
<tr>
<td>5</td>
<td>0.5728</td>
<td>0.5115</td>
<td>0.5001</td>
</tr>
<tr>
<td>6</td>
<td>0.5884</td>
<td>0.5729</td>
<td>0.5561</td>
</tr>
<tr>
<td>7</td>
<td>0.3247</td>
<td>0.1604</td>
<td>0.1751</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

In our research edge detection methods that are explain previously are applied on seven different images in order to analyze the performance of these methods and discover the best one. The images were selected so they contain areas of fine details as well as areas of consistent colors. The 7 images and their results can be seen in figures 3 to 9. We conclude that the Jacobian method produce a thick and disconnected edge with all operators Sobel, Prewitt and Log. While the least square method produce edges that are much thicker but continuous. The good performance was found when using YCbCr method, the edges are sharpen, continuous, and not thickness. They are similar with Sobel and Prewitt operators but with some missing edges while it is better with Log operator.

Table two summaries the performances of the different methods according to the computation complexity, noises immunity, and lines, corners, and curve detected.

<table>
<thead>
<tr>
<th>Edge Detection Method</th>
<th>Computation Complexity</th>
<th>Noises Immunity</th>
<th>Lines, Corners, and Curves Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Least Square</td>
<td>Complex</td>
<td>Very Sensitive</td>
<td>Thickness lines, corners, and curves.</td>
</tr>
<tr>
<td>YCbCr-Sobel</td>
<td>Less Complex</td>
<td>Low Sensitive</td>
<td>Detect outlines (continuous Boundaries) but missing the inners ones.</td>
</tr>
<tr>
<td>YCbCr-Prewitt</td>
<td>Less Complex</td>
<td>Low Sensitive</td>
<td>Detect outlines (continuous Boundaries) but missing the inners ones.</td>
</tr>
<tr>
<td>YCbCr-Log</td>
<td>More Less Complex</td>
<td>Low Sensitive</td>
<td>Detected inner and outlines.</td>
</tr>
<tr>
<td>Jacobian-Sobel</td>
<td>Much More Complex</td>
<td>Sensitive</td>
<td>Thick lines and some breakouts.</td>
</tr>
<tr>
<td>Jacobian-Prewitt</td>
<td>Much More Complex</td>
<td>Sensitive</td>
<td>Thick lines and some breakouts.</td>
</tr>
</tbody>
</table>
Jacobian-Log More Complex Less Sensitive Thick lines, lot of breakouts and missing corners.

ACKNOWLEDGMENT

We would like to thank all who help us in preparing this research. Their help is highly appreciated.

REFERENCES


Designing An Efficient Three Phase Brushless Dc Motor Fuzzy Control Systems (BLDCM)

Rafid Ali Ridha Ibrahim
Department of Physics
University of Kirkuk /College of Science
Kirkuk, Iraq
ibrahim_aslanuz@yahoo.com

Inas Bahaa Abedalrazzaq Deaibil
Department of electrical engineering
University of Kirkuk /College of Engineering
Kirkuk, Iraq
inasrafed@yahoo.com

DOI: 10.24086/cocos17.05

Abstract—In this paper presented a model of three phase BLDC motor. Also presented the construction and operation also derived the state space model of brushless Dc motor. Matlab/simulink models are derived to observed and analyzed the dynamic characteristics of the BLDC motor speed, torque , currents and voltages of the inverter components. Fuzzy control presented in this paper.

Keywords-component; BLDC Motor, FLC control, PWM Pulse Width Modulation

I. INTRODUCTION

Brushless Direct Current (BLDC) motors are among the motor types, which are becoming popular in recent years. The stator of a BLDC motor consists of stacked steel laminations[1],[2]. The windings are placed in the slots that are axially cut along the inner periphery or around the stator. The rotor is made of permanent magnets and can vary from two to eight pole pairs with alternating south poles and north poles. The stator windings should be energized in a sequential order in order to operate the BLDC motor properly. Hence it is necessary to know the rotor position in order to understand the winding to be energized at a specific time instant. In the BLDC motor, power transistors are used for changing the polarity, which is performed by switching the transistors in synchronization with the rotor position. BLDC motors often include either internal or external position sensors to sense the actual rotor position.

In a traditional DC motor (brushed DC motor), the brushes make mechanical contact with a set of electrical contacts on the rotor. These contacting materials are called as commutator. This mechanical contact causes an electrical conduction between the armature coil windings and the DC electrical source[3],[4]. The stationary brushes contact with different sections of the rotating commutator as the armature rotates on its axis. The brushes and the commutator system forms a set of electrical switches, each firing in sequence, such that electrical power always flows through the armature coil closest to the stationary stator permanent magnet.

In a BLDC motor, the permanent magnets rotate and the armature coils remains static[5]. The problem is how to transfer current to a moving armature. Replacing the commutator assembly with an intelligent electronic controller solves this problem. The controller performs the same power distribution observed in a brushed DC motor. However BLDC use a solid-state circuit instead of a mechanical commutator. BLDC motor has a trapezoidal back-EMF and rectangular stator currents are necessary to produce a constant electrical torque. Usually hysteresis or pulse width modulated (PWM) current controllers are used to maintain the actual currents as close as possible to the rectangular reference values[6], [7]. Although some steady-state analysis has been performed, the design of the BLDC motor servo system usually requires a long time trial and error process, and fails to exhibit an improvement in the performance. In practice, the design of the BLDC motor drive requires some complex tasks to be completed such as devising of control scheme, modeling, simulation and parameters adjustment. The proportional integral (PI) controllers are generally suitable for the linear motor control and they have been widely proposed for BLDC motors. But in practice, BLDC motors have many non-linear factors imposed by the driver and the load causing a decrease in the performance. In order to achieve desired level of performance the motor needs appropriate speed controllers and that is only possible with fine-tuning of controller parameters. Usually the speed control is achieved by using PI controller in case of permanent magnet motors. In industry, conventional PI controllers are preferred due to ease of implementation and as they possess simple control structure. The drawback of PI controllers arises when there are some control complexities like nonlinearities, parametric variations and load disturbances. Moreover PI controllers need precise linear mathematical models, however the permanent magnet BLDC machine has a nonlinear model, hence the linear PI may no longer be suitable.

The Fuzzy Logic (FL) approach applied to speed control leads to an improved dynamic behavior of the motor drive system.
and they can be easily implemented for disturbance like load. Fuzzy logic controller (FLC) provides an improvement in the quality of the speed response. Most of these controllers use mathematical models and are sensitive to parametric changes. These controllers are inherently robust to load disturbances. In addition, FLCS could be easily implemented. Due to these properties it is designed to use a FLC for the BLDC motor.

II. BLDC MOTOR MATHEMATICAL MODEL

A. Principal Construction BLDC Motor

BLDC motor has two important components: the rotor part and the stator part. BLDC motor can be categorized as DC motor that is turning inside out, so that the armature is on the stator side and the permanent magnet is on the rotor side. It can also be categorized as a permanent magnet AC motor whose torque-current characteristics resembles the DC motor. In a BLDC motor, electronic commutation is used instead of commutating the armature current using brushes. Besides, as the armature lie on the stator, it is easier to conduct the heat produced in the motor away from the windings hence the cooling facility of the motor is provided automatically.

In BLDC motors it is important to precisely determine the position of the rotor since the commutation is performed electronically due to the rotor position. The position of the rotor may be sensed using optical position sensors. Optical position sensors consist of a light source and phototransistors’ revolving shutters. The output of an optical position sensor is generally a logical signal.

B. Architecture of BLDC System

The block diagram of a BLCD motor control system is shown in Figure 1. The block diagram contains four main parts. These parts are the power converter, controller, motor and sensors.

In order to operate the BLDC motor the controller needs feedback information about the rotor position[9,10]. The controller generates signals, which drive the power converter by using a pulse width modulation (PWM) modulator. The internal block diagram of the power converter and controller is shown in Figure 3. In BLDC motor the rotor speed and supplied voltage are directly proportional. In a PWM controller, the PWM duty cycle controls the voltage [8]. When the voltage is applied, a current flows through the windings of the motor and this current generates torque in order to spin the motor. The motor can spin either in clockwise or counterclockwise direction depending on polarity of the applied voltage. The sensors are used to determine the rotor position and this information is also sent to the controller.

C. BLDC Drives Operation with Inverter

The circuit diagram of a BLCD motor with controller and power source inverter is shown in Figure 4. The inverter in self-control mode acts as an electronic commutator. It receives the switching logical pulse from the position sensors[11]. This kind of motor drive is known as an electronically commutated motor. Mainly the inverter can work by using the following two modes

- (2π/3) angle switch-on mode
- Voltage and current control PWM mode
III. BLDC MOTOR DYNAMIC MODEL

In Figure 5, the BLDC motor electrical model with voltage source inverter is shown. In this model the motor is connected to the output of the inverter, and a constant voltage is supplied to the terminals of the inverter. While constructing the model it is also assumed that there are no power losses in the inverter and the windings of the motor[12].

We can write the phase voltage equations of BLDC motors as follow:

\[ V_a = R_a I_a + L_a \frac{dI_a}{dt} + M_{ab} \frac{dI_b}{dt} + M_{ac} \frac{dI_c}{dt} + e_a \]

\[ V_b = R_b I_b + L_b \frac{dI_b}{dt} + M_{ba} \frac{dI_a}{dt} + M_{bc} \frac{dI_c}{dt} + e_b \]

\[ V_c = R_c I_c + L_c \frac{dI_c}{dt} + M_{ca} \frac{dI_a}{dt} + M_{cb} \frac{dI_b}{dt} + e_c \] (1)

Neglecting the mutual inductance values (M) from the Equations 2, 3 and 4 we obtain:

\[ V_a = R_a I_a + L_a \frac{dI_a}{dt} + e_a \] (5)

\[ V_b = R_b I_b + L_b \frac{dI_b}{dt} + e_b \] (6)

\[ V_c = R_c I_c + L_c \frac{dI_c}{dt} + e_c \] (7)

We can combine Equations 5, 6 and 7 in a matrix as follow:

\[
\begin{bmatrix}
V_a \\
V_b \\
V_c
\end{bmatrix} =
\begin{bmatrix}
R & 0 & 0 \\
0 & R & 0 \\
0 & 0 & R
\end{bmatrix}
\begin{bmatrix}
I_a \\
I_b \\
I_c
\end{bmatrix} +
\begin{bmatrix}
L_a \\
L_b \\
L_c
\end{bmatrix} \frac{d}{dt} \begin{bmatrix}
I_a \\
I_b \\
I_c
\end{bmatrix} +
\begin{bmatrix}
e_a \\
e_b \\
e_c
\end{bmatrix} \tag{8}
\]

Using equation (8) we can also find:

\[ V_{ab} - e_{ab} = R(I_a - I_b) + L \frac{d}{dt}(I_a - I_b) \] (9)

\[ V_{bc} - e_{bc} = R(I_b - I_c) + L \frac{d}{dt}(I_b - I_c) \]

\[ V_{ca} - e_{ca} = R(I_c - I_a) + L \frac{d}{dt}(I_c - I_a) \]

Defining the loop current as I1, I2 and I3 we can also write

\[ I_a = I_1 - I_3 \]

\[ I_b = I_2 - I_1 \]

\[ I_c = I_3 - I_2 \] (10)

In figure 6 generation the three phase current Ia, Ib, Ic is show.

![Figure 6 Block diagram for three-phase currents.](image-url)
As only two phases are exited through a conduction period
Equation in 9 can be rewritten as,

\[
V_{ab} - e_{ab} = 2RI_1 + 2L \frac{dl_1}{dt}
\]
\[
V_{bc} - e_{bc} = 2RI_2 + 2L \frac{dl_2}{dt}
\]
\[
V_{ca} - e_{ca} = 2RI_3 + 2L \frac{dl_3}{dt}
\]

(11)

In terms of functionality BLDC motors are generally put in the
category of Permanent Magnet Alternating Current (PMAC)
motors. PMAC motors can be grouped into two types. The
first type is represented as permanent magnet synchronous
motor (PMSM). This motor produce sinusoidal back-EMF and
it must be supplied with sinusoidal current / voltage source.
The second type is BLDC motor and it has trapezoidal back-
EMF. The back-EMF voltage is produced over the windings
of the motor, while the motor is rotating. The polarity of back-
EMF is in reverse direction compared to the corresponding
phase voltage. Basically back-EMF depends on three factors:
magnetic field generated by rotor magnets, mechanical
angular velocity of the rotor and the number of turns in the
stator windings. Hence, the produced trapezoidal back-EMFs
for each phase are functions of the rotor position, and
mathematically they can be written as[13-14]:

\[
e_a = f_a(\theta)K_eW_m
\]
\[
e_b = f_b(\theta)K_eW_m
\]
\[
e_c = f_c(\theta)K_eW_m
\]

(12)

In Equation 12, \( \theta \) represented the rotor electrical position, \( W_m \)
represents the rotor mechanical speed, \( f_a(\theta) \), \( f_b(\theta) \) and
\( f_c(\theta) \) are the functions of rotor position and \( K_e \) is the motor voltage
constants for each phase. The modeling of the back-EMF
waveforms is implemented according to the assumption that
all three phases have identical trapezoidal periodical back-
EMF waveforms with 120 degrees phase difference between
each of them. The functions of the rotor position \( f_a(\theta) \), \( f_b(\theta) \) and
\( f_c(\theta) \) in a single period can be represented using the equations below:

\[
f_a(\theta) = \begin{cases} 
\left( \frac{6}{\pi} \right) \theta & 0 < \theta < \frac{\pi}{6} \\
1 & \frac{\pi}{6} < \theta < \frac{5\pi}{6} \\
-\left( \frac{6}{\pi} \right) \theta + \pi & \frac{5\pi}{6} < \theta < \frac{7\pi}{6} \\
-1 & \frac{7\pi}{6} < \theta < \frac{11\pi}{6} \\
\left( \frac{6}{\pi} \right) \theta + \frac{11\pi}{6} & \frac{11\pi}{6} < \theta < 2\pi 
\end{cases}
\]

(13)

\[
f_b(\theta) = \begin{cases} 
\left( \frac{6}{\pi} \right) \theta & 0 < \theta < \frac{\pi}{2} \\
1 & \frac{\pi}{2} < \theta < \frac{5\pi}{6} \\
-\left( \frac{6}{\pi} \right) \theta + \pi & \frac{5\pi}{6} < \theta < \frac{9\pi}{6} \\
-1 & \frac{9\pi}{6} < \theta < \frac{11\pi}{6} \\
\left( \frac{6}{\pi} \right) \theta + \frac{11\pi}{6} & \frac{11\pi}{6} < \theta < 2\pi 
\end{cases}
\]

(14)

\[
f_c(\theta) = \begin{cases} 
\left( \frac{6}{\pi} \right) \theta & 0 < \theta < \frac{\pi}{2} \\
1 & \frac{\pi}{2} < \theta < \frac{5\pi}{6} \\
-\left( \frac{6}{\pi} \right) \theta + \pi & \frac{5\pi}{6} < \theta < \frac{9\pi}{6} \\
-1 & \frac{9\pi}{6} < \theta < \frac{11\pi}{6} \\
\left( \frac{6}{\pi} \right) \theta + \frac{11\pi}{6} & \frac{11\pi}{6} < \theta < 2\pi 
\end{cases}
\]

(15)

\( f_a(\theta) \), \( f_b(\theta) \) and \( f_c(\theta) \) can take values between 1 and -1.

We know that the torque produced per phase is directly
proportional with the phase current and back-EMF and
inversely proportional with the mechanical angular velocity of
the motor. Hence torque produced at each phase can be written
as:

\[
T_a = \frac{e_a}{w_m}
\]
\[
T_b = \frac{e_b}{w_m}
\]
\[
T_c = \frac{e_c}{w_m}
\]

(16)

The total electromagnetic torque is the result of summation of
the torques produced at each phase. Thus we obtain,

\[
T_e = T_a + T_b + T_c
\]

(17)

In Equation 17, \( T_e \) is the total electromagnetic torque. The
equation of motion for the BLDC motor can be written as,

\[
\frac{dw_m}{dt} = \frac{1}{J} (T_e - T_1 - B W_m)
\]

(18)

In Equation 18 \( T_1 \) is the load torque, \( B \) is the damping constant
and \( J \) is the moment of inertia of the motor. The relation
between the mechanical angular speed of the motor and the
electrical angular frequency of the motor depends on the
number of poles found on the motor and it can be written as,

\[
W_r = \frac{p}{2} W_m
\]

(19)

In Equation (19), \( w_s \) is the electrical angular frequency (speed)
of the motor and \( p \) is the number of poles. In order to find the
rotor position vector \( \theta \), we can use Equation (2.22) and the
figure 7 show who we obtain (theta, \( I_{max} \), \( W_r \)).

\[
\frac{d\theta}{dt} = W_r
\]

(20)
The mechanical angular speed of the motor is controlled by a control signal, which is the reference torque value $T_{\text{max}}$ produced by the controller. This control signal $T_{\text{max}}$ is converted to the current value $I_{\text{max}}$ (the reference current value) by the torque equation

$$I_{\text{max}} = \frac{T_{\text{max}}}{K_t}$$

In Equation (21) $K_t$ is the torque constant of the motor.

IV. FLC CONTROLLER

In this section instead of using P or PI controller we decided to use FLC to stabilize the BLCD motor speed. In order the see the efficiency of the FLC we used two different rule base structures. These rule base structures are given at Table 1 and 2.

In the first simulation the rule-base structure in Table 1 is used. The normalization factors are taken as $N_{e_1} = 1/220$, $N_{e_2} = 1/5000000$ and $N_u = 1500$. As the result of the simulation the mechanical angular speed profile shown in Figure 8 is obtained.

In the second simulation the rule-base structure in Table 2 is used. The normalization factors are taken as $N_{e_1} = 1/220$, $N_{e_2} = 1/5000000$ and $N_u = 1500$. As the result of the simulation the mechanical angular speed profile shown in Figure 11 is obtained.

From Figure 11, we obtained the following performance indices:

- There is no overshoot in the response, $t_r = 0.0124$ second,
- $w_{m,ss} = 399.91$, $t_s = 0.0119$. The equivalent torque and the Imax graphs for this simulation are shown in Figure 12 and 13 respectively. As we observe there is not so much difference between these performance indices of these two FLC simulations however the steady state value of the second simulation is slightly better the first simulation.
V. CONCLUSION

BLDC are used replacing DC motors in different application. These applications like steering wheel, pumps, and blowers. In this thesis a Matlab/simulink model for BLDC motor drives is proposed. We implemented Fuzzy controller (FLC). Also this simulink allows as to see many dynamic characteristics such as mechanical angular velocity, voltages, mechanical torque phase currents. We can conclude that FLC is the best method because desired speed and torque values could be reached in a short time and we take four indices to show the different between the controller .these indices are: the comparison of the steady state value and the reference set point value of the mechanical angular speed , maximum overshoot value, rise time (tr) and the fourth one is the settling time value (ts) . This reason FLC used widely in industrial applications in comparison with other controller.

REFERENCES

Power Consumption Assessment in Mobile Ad-Hoc Network’s Routing Protocols

Mohamad T. Sultan
Department of Computer Science, Cihan University, Erbil, KRG, Iraq

Salim M. Zaki
Department of Computer Science, Cihan University, Erbil, KRG, Iraq

DOI: 10.24086/cocos17.07

Abstract—Traditional routing protocols in mobile ad hoc networks (MANETs) face the high-energy resources consumption due to process of route discovery. In a MANET, a mobile node consumes its power mainly because of message communication and message processing. The power consumption of a mobile node for communication is the highest and the dominant in comparison to what a node consumes for other tasks. In this paper we evaluate the performance of three main traditional protocol of MANET. A discussion and comparison highlighting their particular merits and drawbacks are also presented. Evaluation study and simulations are performed for analysis and investigation of results.

Keywords: MANETs; Routing protocols; Ad-hoc networks.

I. INTRODUCTION

The advent of wireless mobile ad-hoc networks (MANETs) has offered an efficient and most importantly cost effective technique to make use of the availability of mobile hosts when no fixed infrastructure is provided. In MANET, the mobile nodes can easily communicate with each other while they are freely moving around in different directions. An ad-hoc network relies entirely on nodes cooperation for forwarding information from data sources to intended destination nodes. Some examples of mobile nodes in an ad-hoc network are laptop computers, smart phones and personal digital assistants that interact directly with each other [1][16]. There are many advantages of such an ad-hoc network which include fast deployment, robustness, efficiency, and inherent support for mobility.

Researchers have become more interested on how to secure MANETs. They have suggested several methods to prevent or reduce the risk of attacks on the mobile ad-hoc networks by using access control key management and trust models mechanisms [1][2]. Energy consumption is a very critical issue in MANET since mobile nodes are often powered by limited battery resources. Thus, network lifetime relies heavily on the energy consumption of nodes. Saving energy is, therefore, critical in order to prolong the lifetime of the network. Figure 1 illustrates the architecture of the Mobile Ad-hoc Network (MANET) protocols.

The authors in [3] have proposed a loop-free energy conserving scheme, which tries to decrease routing, and storage overhead to provide optimization of resources use in large-scale networks. The researchers in [4] have found reactive protocols such as DSR; AODV behaved more efficient than DSDV and showed superior performance than TORA. In [5] the authors have investigated AODV based algorithm with less energy consumption during route founding by establishing routes that are lower congested than the others. The traditional routing algorithms lack energy awareness of the nodes in the network. Therefore, in next sections we will analyze and evaluate the protocols to show their performance in terms of energy consumption.

II. MANET ROUTING PROTOCOLS

Several routing protocols for ad-hoc networks have been proposed. The two main basic roles of MANET routing protocols are the selection of path and delivering data packets accurately to the right target. MANET routing protocols can be classified into three different categories which are table-driven routing protocols (proactive), on-demand routing protocols (reactive) and hybrid routing protocols [6][15]. In the following sub-sections, the proactive and the reactive routing approaches will be discussed.

A. Table-Driven Routing Protocols (Proactive)

The table-driven routing protocols always try to keep consistent up to date routing data for every node in the network. These protocols attempt to maintain accurate
routing information of the complete network at all times. Every node in the network keeps the routing information by maintaining one or more routing tables. The nodes usually try to revitalize the information about the target nodes by updating the routing tables. The routing protocol adapts to the sudden changes in topology by broadcasting network updates whenever changes occur [6]. In the following section an explanation of OLSR routing protocol will be presented.

1) Optimized Link State Routing (OLSR)

In OLSR all nodes have routing table for keeping the routing information to every other node in the network to provide a route to the destination immediately when desired [7]. In OLSR routing protocol, one of the most essential key concepts used is the use of multipoint relays (MPRs). The main purpose of the MPRs is to forward the broadcast messages in the network. The traditional link state protocol broadcast mechanism is not used in OLSR. This is because in OLSR only partial link state information is distributed where the content of the broadcast packets is only about MPRs rather than all the detailed link state information [8].

The mobile nodes select the MPRs amongst their surrounding neighbors and then rebroadcast only those messages that are received from nodes who selected it as an MPR. OLSR mainly uses two kinds of control messages. The first one is the periodic HELLO messages while the second type is the Topology Control (TC) messages. The HELLO messages are used for discovering the information about the link status or in other words it carries out the task of neighbor detecting. The second type, which is the Topology Control (TC) messages are used for the purpose of information declaration about the multipoint relay. OLSR protocol is mainly appropriate for large and dense networks for the reason that the technique of multipoint relays performs well in this environment [7][8]. Figure 2 below shows MPR selection in OLSR routing protocol.

![Figure 2. Multipoint relays in OLSR routing protocol](image)

B. On-Demand Routing Protocols (Reactive)

On-demand protocols generate routes only when there is a request to send data. This approach is totally different than that of table-driven routing. Routing information about the mobile nodes is not maintained by protocols instead the route request is initiated only when needed. When the source nodes need to start a route to the target, at this time the route is being initiated to serve the request of the source nodes [6][9].

1) Ad-hoc On-Demand Distance Vector (AODV)

AODV is developed based on the DSDV routing algorithm [6][10]. It is categorized as a pure reactive routing protocol scheme. When there is a route required in the network, AODV will execute route discovery process to find the route to the desired destination. As soon as a route is generated in the network, it is maintained as long as it is still needed using a route maintenance process. Each mobile node keeps the routes that have been discovered in its routing table. However a routing table entry expires if it is no longer being used or has exceeded the expiration period which has been pre-identified earlier. AODV has three essential messages which are the Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) [6]. The RREQ message contains information such as the IP address of the source and destination nodes, current sequence number, broadcast ID and latest sequence number for the destination known to the source node. In response to the request message the mobile nodes send back RREP message to the source node. This reply message contains the information that the source node needs with the valid route. However, when there is a problem in the network another procedure is used which is the RERR message. This message holds a list of all of the unreachable destinations in the network. AODV is a reactive on-demand routing protocol, despite the fact that it still employs some characteristics of the table-driven routing approach. AODV is a good choice for routing in the case when the network is dynamically changing. This protocol combines the motivating features of DSR and DSDV routing in a way that it employs the idea of route discovery and route maintenance like DSR routing protocol and in the same time it makes use of the sequence numbers and transmitting of periodic hello messages from DSDV. The use of destination sequence numbers guarantees loop-free routes and help to detect available fresh routes which allow the source nodes to discover new routes every time[11].

2) Dynamic Source Routing (DSR)

DSR is an independent routing protocol which can be described as a completely self-configuring self-organizing routing protocol [12]. To improve the discovery process in the network, routes caches are kept at the mobile nodes and those caches are frequently updated. DSR involves no periodic data packets within the network of any kind at any
level. For instance, there is no periodic routing advertisement, neighbor detection or link status sensing packets to be used in DSR, and it does not depend on any underlying protocol for those tasks. DSR has two core mechanisms that are route discovery and route maintenance [13]. Once any mobile node within the network desires to send a data message to a particular destination, it initially broadcasts a route request (RREQ) packet. The neighbor and surrounding nodes, which lay in the range of transmission of the source node, receive that RREQ packet and add their own address to it and they rebroadcast it again in the network. If the discovery procedure is successful, the source initiator obtains a response data packet that shows the series of nodes over which the destination could be reached. The route request packet therefore has a record field accumulating a list of nodes visited for the duration of propagation of the query in the network. DSR routing protocol has many benefits. For instance, it does not employ periodic route advertisement which leads to saving in network bandwidth as well as reduction in power consumption. DSR has a faster route recovery than many other reactive protocols as well. However, the limitation of this protocol is that the benefit of caching routes for large networks and higher mobility may become not that useful [12][14].

III. SIMULATION ENVIRONMENT

This section provides the details of the simulation environment used in this paper. The entire simulation work is conducted and implemented on a Linux (Ubuntu distribution) operating system. The simulation is done with the help of NS-2 simulator. NS-2 deals efficiently with network's core components and it provides the complete vision of the network construction this includes routing protocols, transport layer protocols, interface queues, as well as link layer components. The simulation environment consists of four different numbers of nodes which are 10, 20, 30 and 50 mobile nodes. Nodes are being generated randomly at random position and Constant Bit Rate (CBR) traffic generators will be used as sources to run the simulation. For this research study the selected mobility model is the Random Waypoint Mobility Model which is one of the most widely used mobility models among the research community. The selected parameters are varied using setdest command in NS-2 [4].

The simulation parameters considered for the performance evaluation of MANET routing protocols are shown in Table I.

<table>
<thead>
<tr>
<th>TABLE I. SIMULATION PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
</tr>
<tr>
<td>Simulation Tool</td>
</tr>
<tr>
<td>Routing Protocols</td>
</tr>
<tr>
<td>Pause Time</td>
</tr>
</tbody>
</table>

IV. SIMULATION RESULTS AND ANALYSIS

The simulation results of each network scenario that presents the performance of the routing protocols with respect to energy consumption are explained in this section. The node density of the simulation network was varied to determine the performance impact of the three routing protocols.

Figure 3 shows the total energy consumed (Joules) by all the nodes involved in transmitting and receiving the control packets by varying the number of mobile nodes in the network. The node density is increased from 10 to 50 nodes within the same network size as each simulation run is performed.

All the routing protocols show an increase in the consumed energy as the number of the mobile nodes increase and the network size become bigger. This is because the mobile nodes in the network have to process all the routing packets. As such, the total power consumption of the network will increase. According to Figure 3, a considerable difference of energy consumption can be noticed as the network size become larger until it reaches to 50 mobile nodes. The performance of the on-demand routing protocol AODV in terms of the energy consumption is quite poor compared to the other on-demand protocol DSR, and this could be mainly due to the
increase in the maintenance process as the number of nodes increase. Although DSR and AODV have the same on-demand behavior but they are still have a bit different routing mechanisms. That is why AODV has superior energy consumption as compared to DSR where maintenance process of AODV can be the main reason of this increase.

The proactive routing protocol OLSR has an average performance compared to the other protocols. From the figure above it can be seen that the energy consumption of both DSR and OLSR routing protocols increases in quite the same pattern with increasing number of nodes below 30; but the gap in energy consumption only start to occur half way through the simulation and start to become higher after 30 mobile nodes. The shortcomings of this aspect of OLSR are caused by the large number of overheads generated between the nodes within a group. However, OLSR did not perform too badly and has consistently better results than AODV. At higher density nodes, DSR routing protocol performs efficiently in consuming less overall system energy and this is because of DSR as an on-demand protocol doesn't have to maintain route to the target if there is no data to be send. That’s why DSR seems to have better performance compared to its counterparts.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we addressed the issues of energy efficient routing in MANET. Mobile nodes in MANET rely on batteries, consequently efficient utilization of battery energy becomes significant and it affects the increase the lifetime of the mobile network. This paper is mainly focused on several routing algorithms proposed for mobile ad-hoc networks (MANETs). The aim of this research work was to evaluate the performance of three prominent MANET routing schemes which are AODV, DSR and OLSR with regard to energy consumption. The purpose of the work is to comprehend the impact of having more nodes within a fixed map of operation on the network’s energy consumed. In general, the on-demand AODV protocol consumed more energy within the network at the beginning of the simulation and it lasted until the end of the simulation. As mentioned earlier AODV routing protocol has shown higher degree of consumed energy than the DSR and OLSR routing in higher density network operation. While DSR uses source routing with longer header, AODV uses hop-by-hop scheme which may not help in consuming lower energy values. It observed generally that increasing number of nodes results in increasing energy consumption in all routing protocols due to routing control packets. It can be noticed of DSR as being more energy efficient than AODV and OLSR in this research and it emerges as a good candidate in conserving the system energy. This work may generally be concluded by addressing the issue of routing in MANETs which is each routing protocol has certain benefits and weaknesses, and is well suited for certain conditions. Therefore choosing an appropriate routing protocol for MANET would produce the highest routing performance in the network.

For future work, we will add more related work of enhanced versions of energy aware routing protocol additionally will vary simulation parameters such as number of nodes and speed of nodes to evaluate the impact of energy consumption.

REFERENCES


Study and Analysis of Students' Works after Graduation from Computer Science Department in Cihan University – Erbil

Reem Jafar Ismail\textsuperscript{1}  
reem_aljanabe@yahoo.com

Omar Talal Hamid\textsuperscript{1}  
omar_talal20022003@yahoo.com

\textsuperscript{1}Computer Science Department  
Cihan University – Erbil  
Erbil- Iraq

DOI: 10.24086/cocos17.06

Abstract— in recent years, the most important problems that face students after graduation in to find job. In this paper, we collect information for graduated students that had been graduated from computer science department - Erbil for the last five years (from 2010 until 2016) including place of work and job title to analyze them. According to the analysis the most three job titles for work is found with a percentage of the students that work in computer science field and work in public or private field. This study is important for both students and university to recognize the difficulties that face students after graduation and to develop the computer science department to meet business market.

Keywords- Graduated students, percentage of students that has employed or not employed, work in computer science field, work in public or private field.

I. INTRODUCTION AND RELATED WORKS

These Computers are now a fact of life. Computers have created a very effective information for management of an organization. This makes it a much-needed tool for every business, daily life, government, entertainment, banking, industry, administration and education. It can be said of all large organizations whether the department government or private, use a computer for a variety of their daily business and it is the fastest growing industries in the world today. Each organization usually has one or more computer systems for data processing tasks or even to use word application. Computers have become part of our lives is essential. Computer plays an important role of in many areas, [1]:

- Business: example is to calculate the salary, to identify the goods sold and are still in stock, to issue and send or receive business statements, letters, invoices and more.

- Financial and Banking: processing data involving fixed deposits, loans, savings accounts, profitability, investments, analysis are among the organizations operating budget.

- Industrial Areas: industry is a lot of benefit from the use of computers and the development of a human machine that 'robot'. Industrial production, for example requires many computers to process data collected from, production schedules, product information, sales, employees and customers.

- Education: computer is important in education from student registration, class scheduling, processing of examination results, students 'and teachers' personal storage can be implemented by a computer with a fast and effective in helping the administration. Now exams results were processed also by computer.

- Medical: clinics and hospitals use computers to store scheduling doctors, nurses, patient records, medical diagnosis, medical research, inventory and purchase of medicines and other personnel.

The fact is computers have become the backbone of society today. Whatever the field, computing has many people taken over the task. It will not only help in the store information, calculations, productivity, detect a decision also to increase efficiency.

The Department of Computer Science specializes in the training of students who want to apply their knowledge of technology in scientific environments (Computer Science) or in the corporate world (Informatics). The department delivers highly trained individuals with technical skills in programming, system analysis and design as well as database management and network. The department is dedicated to producing top quality graduates, equipped for a professional career in national and international companies [2].

The aim of this research is to study and analysis the students' works after graduation from computer science department in Cihan University - Erbil. This study is important for both students and university to recognize the difficulties that face students and to develop the department.

In Egypt, the faculty of computer and information in Assiut University find statistics for graduated students that had worked. In 2012-2013, 7% of total graduated students had worked while 19% has no work and 70% were unknown. In
of total graduated students had worked while 33% has no work and 65% were unknown [3].

In United State (New Your), computer science field in Hofstra University find the career outcomes rate in 2014-2015, and the employment rate – employed full or part time (Hofstra surveys, LinkedIn, and faculty feedback) which was 100% [4]. Also in Pennsylvania, University of Pennsylvania the career services collect surveys in the school of engineering and applied science were about 69% and 78% had been employed in 2013-2014 and 2014-2015 respectively [5].

This paper is organized as follows: section II gives a detailed explanation about the methodology especially in data collection, section III Results and Analysis, section V and IV give discussion and conclusions including recommendation and future works in section VI and VII, respectively.

II. METHODOLOGY

The data used in this research study were based on surveys of computer science graduates of Cihan University-Erbil.

The student information was collected by calling each one with mobile or contact with e-mail. Table (I) shows the total number of students that had been graduated from computer science department Cihan University-Erbil from (2010-2016). Table (II) summarizes the most important attributes for each student that supplies our objective, where each student has a name, place of work, job title and whether he/ she is working in government or private sector for all daytime and evening study, about 598 records are saved in the database. Microsoft Excel 2016 is used as software application to record the information in Table (I to VI) and find the necessary statistics.

### TABLE I TOTAL NUMBER OF STUDENTS THAT HAD BEEN GRADUATED FROM (2010-2016).

<table>
<thead>
<tr>
<th>Study Session/ Year</th>
<th>Total Number of students</th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daytime 2010-2011</td>
<td>121</td>
<td>75</td>
<td>46</td>
</tr>
<tr>
<td>Daytime 2011-2012</td>
<td>123</td>
<td>72</td>
<td>51</td>
</tr>
<tr>
<td>Daytime 2012-2013</td>
<td>91</td>
<td>57</td>
<td>34</td>
</tr>
<tr>
<td>Evening 2012-2013</td>
<td>21</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>Daytime 2013-2014</td>
<td>141</td>
<td>75</td>
<td>66</td>
</tr>
<tr>
<td>Evening 2013-2014</td>
<td>20</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>Daytime 2015-2016</td>
<td>54</td>
<td>32</td>
<td>22</td>
</tr>
<tr>
<td>Evening 2015-2016</td>
<td>27</td>
<td>22</td>
<td>5</td>
</tr>
</tbody>
</table>

### TABLE II SAMPLE OF REAL INFORMATION FOR EACH STUDENT THAT HAD BEEN GRADUATED FROM (2010-2016).

<table>
<thead>
<tr>
<th>Place of Work</th>
<th>Job Title</th>
<th>Government Sector or Private Sector</th>
<th>Graduated Year</th>
<th>Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nawroz Telecom</td>
<td>IT</td>
<td>Private</td>
<td>2010-2011</td>
<td>Morning</td>
</tr>
<tr>
<td>Cihan University - Erbil</td>
<td>Lab Assistant</td>
<td>Private</td>
<td>2010-2011</td>
<td>Morning</td>
</tr>
<tr>
<td>Ministry of Education</td>
<td>Teacher</td>
<td>Governmen t</td>
<td>2010-2011</td>
<td>Morning</td>
</tr>
<tr>
<td>Bank</td>
<td>IT</td>
<td>Private</td>
<td>2011-2012</td>
<td>Morning</td>
</tr>
<tr>
<td>Asia Cell Telecom</td>
<td>IT</td>
<td>Private</td>
<td>2012-2013</td>
<td>Morning</td>
</tr>
<tr>
<td>Ministry of Interior</td>
<td>IT</td>
<td>Governmen t</td>
<td>2013-2014</td>
<td>Morning</td>
</tr>
<tr>
<td>Jobless</td>
<td>-</td>
<td>-</td>
<td>2014-2015</td>
<td>Morning</td>
</tr>
<tr>
<td>Cihan University - Erbil</td>
<td>Lab Assistant</td>
<td>Private</td>
<td>2015-2016</td>
<td>Morning</td>
</tr>
<tr>
<td>No answer</td>
<td>-</td>
<td>-</td>
<td>2012-2013</td>
<td>Evening</td>
</tr>
<tr>
<td>Erbil International Airport</td>
<td>IT</td>
<td>Governmen t</td>
<td>2013-2014</td>
<td>Evening</td>
</tr>
</tbody>
</table>

III. RESULTS AND ANALYSIS

After collecting data and information, some students had been answer our calls and give us their information and other could not be reached because they didn't answer or there was a problem in contact number. Table (III) summarizes a percentage of students who answer call compared to other students that didn't answer for each year (2010-2016) and fig. (1) shows the total percentage through five years for those who has answer our call or didn’t answer.

### TABLE III PERCENTAGE FOR STUDENTS WHO ANSWER CALL COMPARED TO OTHER STUDENTS THAT DIDN'T ANSWER FOR EACH YEARS (2010-2016).

<table>
<thead>
<tr>
<th>Study Session/ Year</th>
<th>Percentage For those who answer call</th>
<th>Percentage for those who didn’t answer call</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daytime 2010-2011</td>
<td>41.32</td>
<td>58.68</td>
</tr>
<tr>
<td>Daytime 2011-2012</td>
<td>39.02</td>
<td>60.98</td>
</tr>
<tr>
<td>Daytime 2012-2013</td>
<td>45.05</td>
<td>54.95</td>
</tr>
<tr>
<td>Evening 2012-2013</td>
<td>57.14</td>
<td>42.86</td>
</tr>
<tr>
<td>Daytime 2013-2014</td>
<td>43.97</td>
<td>56.03</td>
</tr>
<tr>
<td>Evening 2013-2014</td>
<td>75.00</td>
<td>25.00</td>
</tr>
<tr>
<td>Daytime 2015-2016</td>
<td>79.63</td>
<td>20.37</td>
</tr>
<tr>
<td>Evening 2015-2016</td>
<td>22.22</td>
<td>77.78</td>
</tr>
</tbody>
</table>
The important point is to find a percentage of graduated students who has work in computer science field or other fields. Table (V) shows percentage of students for each year who has work in computer science field or other fields and fig. (3) shows total percentage of students through five years for those who has work in computer science field with 52% compared with 48% for other fields.

**TABLE V  PERCENTAGE OF STUDENTS FOR EACH YEAR WHO HAS WORK IN COMPUTER SCIENCE FIELD OR OTHER FIELD.**

<table>
<thead>
<tr>
<th>Study Session/ Year</th>
<th>Computer Science field</th>
<th>Other field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daytime 2010-2011</td>
<td>54.55</td>
<td>45.45</td>
</tr>
<tr>
<td>Daytime 2011-2012</td>
<td>51.72</td>
<td>48.28</td>
</tr>
<tr>
<td>Daytime 2012-2013</td>
<td>50.00</td>
<td>50.00</td>
</tr>
<tr>
<td>Evening 2012-2013</td>
<td>45.45</td>
<td>54.55</td>
</tr>
<tr>
<td>Daytime 2013-2014</td>
<td>65.52</td>
<td>34.48</td>
</tr>
<tr>
<td>Evening 2013-2014</td>
<td>69.23</td>
<td>30.77</td>
</tr>
<tr>
<td>Daytime 2015-2016</td>
<td>14.81</td>
<td>85.19</td>
</tr>
<tr>
<td>Evening 2015-2016</td>
<td>16.67</td>
<td>83.33</td>
</tr>
</tbody>
</table>

Fig. (4) Shows percentage of students through five years for those who has work in different fields. So below is a list of companies and ministries who have hired our alumni that graduated between 2010-2016: Ministry of Health, Oil Ministry, Telecommunications Company, Ministry of Education, Ministry of Defense, Airline Office, Ministry of Electricity, Banks, Study, Employee Officer, Interior Design, IT Staff, Ministry of Transportation, Ministry of Higher Education.
IV. DISCUSSION

The following is a list of jobs that the alumni of computer science from Cihan University - Erbil can work with according to the current curriculum of department:

- IT
- System analysis
- Project Manager
- Programmer with: C++, Java, Visual Programming, C#
- Web developer using: CSS3, HTML5, and PHP
- Computer network
- Database (MS Access and MySQL)
- Information security
- Multimedia
- Lab Assistant
- Windows and UNIX operating system
- Microsoft office applications
- Multimedia and Photoshop

The following is a list of fields to work with which is specialist in computer science that the alumni of computer science from Cihan University - Erbil cannot work with, like:

- Video Game Designer
- Mobile Developer
- Cloud Computing
- Micro controllers programming
- Embedded systems
- Python programming

This is because those topics is not included in the curriculum of department.

Where do our alumni go? This question could be answered form the list below, which gives a sampling for companies that have hired our alumni who graduated between 2010-2016:

- Ministry of Health
- Oil Ministry
- Telecommunications Company
- Ministry of Education
- Ministry of Defense
- Airline Office
- Ministry of Electricity
- Banks
- Study
- Employee Officer
- Interior Design
The limitation of this study is that the information that we use is changing, since some graduated students may find or leave job recently through the time of our study. In addition, the contact for most of graduated students are difficult to reach because some student did not answer on mobile or the mobile number was close.

4. Computer science student could work in different fields according to the results that we find in fig. (3) Which shows a percentage of students through five years for those who has work in different fields.

5. According to the current economical situation in the region especially the last two years, the chance of employment in private companies is more that those in government sector even with the tremendous reduction of private companies in the region, as shown in fig. (5 and 6).

6. This study is very important and unique in the region, we try to find the same study to compare with but there is not enough information found to compare with.

7. Each department in all universities must analysis the alumni employment to develop their department and undergraduate students.

VI. RECOMMENDATION

1. Curriculum development to increase the chance of employment for graduated students especially:
   Video Game Designer Jobs, Mobile Developer Jobs, Cloud Computing Jobs.

2. Interest in the summer training for undergraduate students to enrich their resumes.

3. Interest in volunteer work during the study to gain practical skills and experience.

4. The importance of self-development for graduated students form computer science department, what you knew today may be useless because of fast evolution of information technology.

5. Indeed, the English language skills, which are the most important skills for the local, regional and international labor markets, must be developed more for alumni.

VII. FUTURE WORK

1. Compares with Cihan University - Duhok and Slymanya when students will graduate within next years.

2. Complete a survey about the graduated student employment that include, for example:
   "When did you find the job, after 3 or 6 months or more?"

V. CONCLUSION

The most job title for work was:
1. Employee officer with 25.28 %, IT Staff with 23.03 % and Telecommunications Company with 15.17 %.
2. According to the results, that we find in table (IV) the students that employed is usually more than those who has not employed through all the five years, which gives us a good indicator.
3. According to the results that we find in fig. (2), the students that has been work in computer science field is more than those who has work in other fields through all the five years.

ACKNOWLEDGMENT

This work has been implemented to the Department of Computer Science Department in the Cihan University - Erbil. The authors wish to acknowledge the help provided by the staff of Computer Science Department in Cihan University in the data collection stage, especially Mr. Aram M., Mr. Mohammad S., Mr. Chawan and Miss Eman Sabah.

REFERENCES


[2] UFS University, Department of Computer Science and Informatics, Undergraduate Programmes, Yearbook 2016.

[3] Assiut University, faculty of computer and information http://www.aun.edu.eg/faculty_computer_information/alumni/graduate1.php


Factors influencing the adoption of Location Based Identification in Kurdistan Regional of Iraq

Sara Muhammad Amin
Computer Science Cihan University
Erbil Iraq
qaradaxi@gmail.com

DOI: 10.24086/cocos17.17

Abstract—This study examines the factors that affect the adoption of Location Based Identification LBI in the developing countries and more specific in Kurdistan Regional of Iraq (KRI). LBI has different names in different countries such as postcode in the United Kingdom and zip code in the United States. As a base model, the Technology Acceptance Model (TAM) and the Decomposed Theory of Planned Behaviour (DTPB) have been used to model the adoption factors of LBI in KRI. The latent variables used in this study are government support (GS), self-efficacy (SE), perceived usefulness (PU), perceived ease of use (PEU), compatibility (COM), Family and friends (FF), attitude (A), subjective norm (SN), perceived behaviour control (PBC) and behaviour intention (BI). A survey was conducted involving a total of 250 respondents. By using these models, the adoption of LBI system by the citizen of KRI has been proven. The results encourage the Kurdistan Regional Government decision makers to develop strategies that will lead to the adoption of LBI system in the region.

Keywords-component; Decomposed theory of planned behaviour (DTPB); Location Based Identification (LBI); Kurdistan Region of Iraq (KRI); Technology acceptance Model (TAM).

I. INTRODUCTION

The evolution of technology innovation in the last few decades has had a major effect on LBI systems in developed countries. LBI has contributed to this technology evolution in many fields as evidenced by mailing systems, satellite navigation systems, government tax collection, online shopping and parcel delivery, tourism and other similar sectors. The reliance on LBI has led to productivity improvement, accelerating services, flexible working practices and hence, many cost savings. In many developed countries, LBI has been successfully utilised in organizing the daily life of society and individuals. Mailing systems, marketing, tax collection and many other activities of government or the private sectors rely on LBI [1].

In KRI where this study was conducted, a new method for LBI (SR_LBI) has been proposed as an alternative to the recently implemented system in Erbil city. SR_LBI technique depends on the direction and distance of any defined point from the city or area centre. The technique works on dividing the area into circular or rectangular zones around the area centre. Then the area divided axially into four main sections (North, South, East and West) based on the available streets in the area. SR_LBI has been explained and discussed as a new method in the literature “Designing a Postcode System for Erbil City Iraq”[2]. The main purpose of proposing this method is due to having three different LBI systems in the main three cities of the KRI. Each of the three current LBI systems are designed by each of the local city Governorates and do not cover the rural areas in the region. In the last decade, LBI systems in the KRI area have been subjected to three consecutive changes without any notion of applying a unique system for the region.

In this study the SR_LBI has been justified against the factors influencing LBI reliance. Both TAM and DTPB models have been used. The purpose of using TAM is to test the system acceptance by the citizens based on the perceived usefulness and ease of the use of LBI. The purpose of using DTPB is to highlight the reasons behind an ineffectiveness of LBI being implemented in KRI. This problem can be addressed using Decomposed Theory of Planned Behaviour (DTPB) as the latent variable of PBC decomposed to government support. The importance of government support is highlighted as an issue in persuading people to use an effective LBI system.

For this project, 250 participants took part in a questionnaire, of which 236 questionnaire forms have been completed fully. The results have been analyzed using IBM SPSS statistic 22 and AMOS graphic. The results show that the data is a reasonable fit against the DTPB model and a better match against the TAM model.

II. MODELS OF BEHAVIOUR

To investigate and examine the factors influencing the acceptance of the technological importance of LBI, several technology-based models have been proposed and developed to study user acceptance, reliance, and usage behaviour. The theoretical technology models utilized to study user acceptance, reliance, and usage behaviour include the Theory of Reasoned Action (TRA) proposed in 1975 by Fishbein and Ajzen, which consists of attitude towards behaviour, subjective norm and behaviour intention[3][4]. The Technology Acceptance Model (TAM) is based on ease of use and
usefulness of the system which affects attitudes towards the behaviour. This leads to a behavioural intention to use any particular system [5][6][7][8]. Further, the Theory of Planned Behaviour (TPB) is an improved version of TRA [9]. TRA is based on attitude and subjective norm. However, TRA, comes with a perceived behaviour control factor, which affects the behavioural intention towards using a system as an external factor [12][13]. The TPB model has been updated by Taylor and Todd into the Decomposed Theory of Planned Behaviour DTPB by specifying indicators for each latent variable. As such, DTPB is a more robust model than TPB [14].

Some research studies investigate the factors affecting non-technology system acceptance and as such, are not based on technology models. LBI as a non-technology system is used in many technology systems such as satellite navigating system, online application (bills payments, shopping delivery), finding tourist attractions and other sectors. Thus the DTPB and TAM are the preferred models for this field. In this study both the computer technology model DTPB [14] and TAM [5] have been used to prove the LBI system acceptance in KRI.

The advantage of DTPB model over the other models is that it identifies specific significant beliefs that may influence system usage [10]. The purpose of proposing this model is to improve the predictive power of that provided by other traditional models. The main improvement of DTPB is presented in terms of an increased explanatory power and a better, more precise, understanding of the antecedents of behaviour when compared with TPB [14]. However, Taylor and Todd argued that if the sole goal is the usage prediction, then TAM might be preferable. The main feature of decomposed TPB is to provide the full understanding of usage behaviour, intention and effective guidance to researchers.

III. RESEARCH MODEL

The proposed model for this project has been designed based on the integration of TAM and DTPB as shown in Fig 1. Fig. 1 shows the proposed model which the research questionnaire. The designed model explains the constructs that have positive or negative effects on people’s attitude toward using LBI. The constructs include: perceived usefulness, perceived ease of use, compatibility, family and friends, self-efficacy and government support as independent variables. The dependent variable constructs include attitude, subjective norm, perceived behavioural control and intention to use. The strength of the hypothesized relationships has been tested and embedded in the proposed model Fig 1. In addition, the robustness of the model in predicting citizens’ intention to adopt LBI in KRI has been confirmed in this study.

Fig. 1 represents the used model including both TAM (the circular variables) and DTPB (as the whole model). TAM consists of perceived usefulness (PU) and perceived ease of use (PEU) as independent variables in addition to attitude towards behaviour (A) and behaviour intention (BI) as depended variables. Based on the TAM latent variables the model can be tested to what extent the LBI system is acceptable and usable by the KRI citizen. However, DTPB consists of ten construct variables in which this research hypotheses (research questions) are based upon. These construct variables include perceived usefulness (PU), perceived ease of use (PEU), compatibility (COM), family and friends (F&F), self-efficacy (SE), government support (GS), attitude (A), subjective norm (SN), perceived behaviour control (PBC) and behaviour intention (BI) as presented in Fig 1. Based on these variables, the LBI acceptance could be investigated.

Based on the quantitative method, an online questionnaire has been designed as shown in Appendix 1. Based on TAM factors (PU and PEU) a number of questions have been prepared. For example, to which extent the LBI system is easy to use and its usefulness. Based on the TAM part of the questionnaire results, the LBI system acceptance has been proved. Moreover, the study uses DTPB factors to produce all the questions of the same questionnaire. In addition to the TAM related questions, the DTPB questions are designed based on compatibility, family and friends, self-efficacy, government support as independent variables and subjective norm, perceived behaviour control as depended variables. Adding government support as an indicator to perceived behaviour control is to highlight this factor as a backbone of successfully implementing the LBI system in KRI. By using the DTPB results the weak reasons behind the inactiveness of LBI is established.

Furthermore, in addition to the demographic questions applied in this study questionnaire, some relative questions have been asked. One of these questions relates to the participant’s preference to choose one address style between two choices; (a proposed alpha-numeric address or an available numeric address in KRI). The results of this questionnaire has been analysed and discussed in Table 1.
Based on the proposed model, which is based on both TAM and DTPB Fig 1, nine different hypotheses have been formulated as presented in Fig 2. The first three hypotheses (H1, H2 and H3) are proposed based on both TAM and DTPB, whilst hypotheses (H4, H5, H6, H7, H8 and H9) are based only on DTPB. The hypotheses and the mathematical equations behind dependent variables have been presented in the following subsections.

A. Attitude (A)

Most information technology acceptance models include a factor of attitude towards behaviour. This attitude examines the positive or negative feelings of individuals towards behaviour intention [10][13]. Based on Taylor and Todd the core constructs of behaviour, as illustrated in equation 1, are attitude toward behaviour (A), subjective norm (SN), and perceived behaviour control (PBC). Based on TAM, attitude is decomposed into perceived usefulness and perceived ease of use as shown in equation (2). While in DTPB attitude will be decomposed into perceived usefulness, perceived ease of use and compatibility as shown in equation (3).

\[ B \equiv B_I = w_1 A + w_2 SN + w_3 PBC \] (1)

\[ A_{TAM} \equiv w_4 PU + w_5 PEU \] (2)

\[ A_{DTPB} \equiv w_4 PU + w_5 PEU + w_6 COM \] (3)

Note: \( w_i \) has been evaluated as a weight for each factor in the questionnaire. In which, the value of \( w_i \) for each question can be determined based on the answer (1 strongly disagree, 2 disagree, 3 neutral, 4 agree or 5 strongly agree).

This decomposition gives more detail about the reasons of feeling positively or negatively towards the system. By improving the system based on these factors PU, PEU and COM the probability of positive attitude will increase and leads towards encouraging the use of the system.

Perceived usefulness and ease of use are important factors for technology adoption determinants in the technology acceptance model [5][11]. In the present study, these factors have been taken into consideration. Davis et al. (1989) defined perceived usefulness as the extent of a person’s belief regarding the effect of using a specific system on her/his job performance [6]. Perceived ease of use is the level of effort needed for using the new system by the user [5]. Further, compatibility is defined as the level of system fit with the potential existing values and experiences [15]. The following hypotheses have been proposed based on attitude toward behaviour.

H1. Attitude has a positive effect on intention to use LBI system.

H2. Perceived usefulness has a positive effect on citizen attitudes toward using of LBI system.

H3. Perceived ease of use has a positive effect on citizen attitudes toward using of LBI system.

H4. Compatibility has a positive effect on citizen attitudes toward using the LBI system.

B. Subjective norms (SN)

Subjective norms refer to “the person’s perception that most people who are important to him/her think he/she should or should not perform the behaviour [3] page 302. A subjective norm is the important factor when the users have limited experience towards developing attitudes. This happens prior to or in the early stages of innovation implementation [14][16]. As such, SN is a combination of both peer influence and superior influence as shown in Equation (4). According to Chua, some groups will potentially influence adoption such as the adopter’s friends, family, and colleagues [17].

\[ SN = w_7 PI + w_8 SI \] (4)

Based on subject norms, the following hypotheses have been formulated.

H5. Subjective norm has a positive effect on citizen behaviour intention to use LBI system.

H6. Family and friends has a positive effect on subjective norm to use LBI system.

C. Perceived behavioural control (PBC)

Perceived Behavioural Control refers to the user’s perception of his/her ability to achieve system usage [14]. The perceived difficulty, as it is related to internal constraints, is one of the most important factors that should be taken into account as evidenced by Sparks et al. [18]. In this study, PBC is evaluated by summation of self-efficacy and government supports as shown in equation (5).

\[ PBC = w_9 SE + w_{10} GS \] (5)

Self-efficacy is a people’s confidence and predictions in their ability to perform a particular behaviour [19]. The adoption of any new system is based on the range of the support provided by the government, which plays an important role in the diffusion of innovation [20]. The following hypotheses are based on PBC.

H7. Perceived behaviour control has a positive effect on citizen’s behaviour intention to use LBI system.

H8. Self-efficacy has a positive effect on perceived behaviour control towards using LBI system.

H9. Government support has a positive effect on perceived behaviour control.
order to answer the research hypotheses discussed in section III. Other than the demographic questions, the responses measure the questions on a five point Likert-scale 1 (strongly disagree), 2 (disagree), 3 (state of unsure or neutral), 4 (agree), and 5 (strongly agree).

A. Sample profile

Google Form has been used to design the online questionnaire and has been published in December 2014. The questionnaire was distributed via professional social media groups, such as overseas postgraduate students, and sent via emails to people who have knowledge of LBI or have used this type of system. Data collection took approximately three months and the last data accepted was at the end of February 2015. The majority of the respondents are either studying or living in countries such as the United Kingdom and Germany where LBI systems are active.

A total of 250 responses were returned of which 236 of them were completely answered and considered in the present study. The participants were composed of 80.5% male and 19.5% female. The age range of 72.9% of the total respondents were between 26 and 35 years old; 15.3% were between 36-45, 10.6% were between 18-25 years old and only 1% were above 56 years of age. 74.2%, of the respondents were MSc/PhD degree holders, 22.9% of them were between 18-25 years old and only 1% were above 56 years old; 15.3% were between 36–45, 10.6% were 46-55, 7.8% were 56-65, 4.8% were 66-75, and only 1% were above 75. 80.5% male and 19.5% female.

B. Measurement Model Test

The data analysis was realized by using structural equation modelling (SEM) to examine the measurement model to assess convergence and hence determine validity. The measurement model has been evaluated in terms of reliability and convergent validity.

Cronbach’s alpha values have been considered to test the data reliability as shown in Table II. The values of Cronbach’s alpha should exceed 0.5 as a minimum acceptable level of data reliability. Most of these values are greater than 0.8 except for Attitude towards behaviour and Perceived behaviour control which are 0.67 and 0.71 respectively.

To ensure that the measures of a given construct should be highly correlated among themselves, a convergent validity factor has been considered. The evaluation in terms of convergent validity has been made, based on the two criteria proposed by Fornell and Larcker [21][23]. The first criteria indicates that the all indicator factor loadings should exceed 0.7 and the second criteria indicates that the average variance extracted (AVE) for each construct should exceed the variance due to measurement error for that construct (i.e., should exceed 0.50). The results, presented in Table II, show that the first criteria has been met as the most exhibited loading factors are higher than 0.7. The only exception is for Attitude towards behaviour as the factor loading is 0.64. Furthermore, the symbol (/) in Table II represent the null value of factor loading because TAM model has only limited factors as discussed in section (II). The AVE results, as shown in Table II, are ranged between 0.54 and 0.93. The minimum value of AVE is greater than variance due to measurement error (0.5). As both mentioned criteria have been met, the convergence validity for the measurement model has been proved.

Table II Measurement analysis results.


C. Structural Model Test

The procedure of fitting the statistical prediction model with the observed data is known as the goodness-of-fit. In other word, the observed data should fit the model prediction. To identify goodness-of-fit, many fit indices have been designed to support structural equation modelling. Five common indices have been used in the present study. These are chi-square/degrees-of-freedom (χ²/df), comparative fit index (CFI), normed fit index (NFI), incremental fit index (IFI), and root mean square error of approximation (RMSEA). Both models, TAM and DTPB, have been compared based on the mentioned measurements as illustrated in Table III. As shown, the fit statistics outcomes of CFI, NFI and IFI for both TAM and DTPB are greater than or equal to 0.9 and RMSEA values are ranged from 0.05 to 0.08, which indicate a good model fit [22][23][24].

Overall, the result of TAM shows a better model fit than DTPB by using the same sample size. This difference is due to reasons, such as higher number of observed variables and existence of government support in DTPB, which are the main sources of measurement error.

Based on the result of the fit indices explained above, TAM gives a better model fit than DTPB with the same sample size. Furthermore, the result of Akaike’s Information Criterion (AIC), 137.15 for TAM and 724.15 for DTPB, is further evidence that TAM has a better model fit than DTPB as the lower value of AIC indicates the better model fit [23][24].

<table>
<thead>
<tr>
<th>Fit indices</th>
<th>Norm</th>
<th>Obtained value TAM</th>
<th>Obtained value DTPB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute indices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scaled CMIN (CMIN/DF)</td>
<td>&gt;1 and &lt;5</td>
<td>2.238</td>
<td>2.334</td>
</tr>
<tr>
<td>Root mean square error of approximation (RMSEA)</td>
<td>&lt; 0.08</td>
<td>0.073</td>
<td>0.075</td>
</tr>
<tr>
<td>Incremental indices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comparative fit index (CFI)</td>
<td>&gt;0.9</td>
<td>0.977</td>
<td>0.928</td>
</tr>
<tr>
<td>Normed fit index (NFI)</td>
<td>&gt;0.9</td>
<td>0.96</td>
<td>0.9</td>
</tr>
<tr>
<td>Incremental fit index (IFI)</td>
<td>&gt;0.9</td>
<td>0.977</td>
<td>0.929</td>
</tr>
<tr>
<td>Parcimonie indices AIC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The lower by comparison</td>
<td>137.15</td>
<td>724.15</td>
<td></td>
</tr>
</tbody>
</table>

D. Hypotheses testing

From the proposed model, the standardized parameter estimation is depicted in Fig. 2. H1 Attitude is significantly and positively influencing behaviour intention to use an LBI system (β=0.32, p=0.01), thus, H1 is supported. The second hypothesis H2 is supported as the results show that the perceived usefulness is significantly and positively affecting attitude toward LBI (β=0.41, p<0.001).

H3 has also been supported as the results (β=0.56, p<0.001) prove that the perceived ease of use is significantly and positively related to attitude to use LBI. Furthermore, H4 is supported as the compatibility is significantly and positively affecting attitude toward using LBI (β=2.78, p<0.005). H5 has been supported, as the subjective norms are significantly and positively influencing behaviour intention to use LBI (β=0.15, p<0.05). Family and friends are significantly and positively affecting subjective norm to use LBI (β=0.62, p<0.001). Self-efficacy, H8, is supported which has significant and positive effect on perceived behavioural control to use LBI (β=0.87, p<0.001). The significant and positive influences of government support (H9) on perceived behavioural control to use LBI, as the final hypothesis, have been supported by the results of (β=0.11, p<0.05).

I. Conclusions and Discussion

The Technology Acceptance Model has been used in the present study to test the acceptance of a nontechnology system such as LBI. Both TAM and DTPB models have been used to examine the adoption of LBI system in KRI. The reasons behind using two different models are to concentrate on the effects of government support (GS) for activating LBI system in KRI by using DTPB and comparing with the results of TAM. Furthermore, TAM focuses on PU and PEU factors that have positive effects on attitude toward using LBI system that gives better results when compared with DTPB. This result shows that the proposed model has a good explanatory power and confirms its robustness to predict the intention of the citizens to accept and use an
LBI system. However, this type of system has been neglected so far due to the absence of government support, which has led to lack of community awareness towards using the LBI in the private sectors. The research hypothesis results show that the p value of GS is less than 0.061 while the overall p value is less than 0.001. Perceived usefulness is found to be a significant determinant in predicting the behavioural intention to use LBI in the both models of TAM and DTPB. This study clearly demonstrated that the perceived ease of use has a significant effect on attitude toward LBI. The results of DTPB show that compatibility, family and friend, self-efficacy, subjective norm and perceived behaviour control have positive effects on attitude towards using the system.

To design an accepted LBI system by KRI citizens, the results of this study can be useful. The designed system, preferred by those who completed the survey, has features of ease of use. The preferred system uses a short code with a constrained number of alpha-numeric characters as described in [2] rather than long series of 13-digit as currently used in KRI. Replacing the classical governmental system, to the modern system is a key factor toward utilising LBI. Community support in terms of awareness and advertisements may help to increase confidence in using LBI in daily life.

Reference

Appendix 1: The questionnaire used in the present study

<table>
<thead>
<tr>
<th>Questions</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perceived Usefulness</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PU1: Using the addressing system would enable me to accomplish my tasks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>more quickly.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PU2: Using the addressing system would make it easier for me to carry out</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>my tasks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PU3: Using the Addressing system in my life increases my productivity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Compatibility Relative advantage</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM1: Using the Addressing system will save time.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM2: Using addressing system allows me to manage my work more</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>effectively.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM3: Using addressing system gives me greater control over my work.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ease of Use</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOU1: Addressing system is easy to learn.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOU2: Addressing system is easy to operate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOU3: Interaction with addressing system does not require a lot of mental</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>effort.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Family and Friends</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FF1: My family would think that I should use Addressing system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FF2: Most people would think that I should use the Addressing system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Efficacy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EF1: I would feel comfortable using the Addressing system on my own.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EF2: I am confident of using addressing system even if I have never used</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>such a system before.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3: I am confident of using addressing system if I have just seen someone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>using it before.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Government Support</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GS1: The government supports using Addressing system in Kurdistan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regional Government.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GS2: Kurdistan government is active in setting up the facilities to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>activate addressing system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Attitude</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A1.: Using the Addressing system is a good idea.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A2.: Using Addressing system is a wise idea.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Subjective Norm</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SN1: People who influence my behaviour would think that I should use the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addressing system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SN2: People who are important to me would think that using the Addressing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system is a wise idea.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Perceived Behavioural Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PBC1: I would be able to use the Addressing system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PBC2: Using the Addressing system is entirely with my control.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Behavioural Intention</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BI1: I plan to use the Addressing system if available.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BI2: I intend to use the Addressing system to send, receive post and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>other applications within the next 3 months if available.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Challenges Smartphone’s Big Data in HealthCare Systems

Mohammed Hussein Shukur¹, Laith R. Fliah² and Aram Mohammed³
Computer Science Department
Cihan University – Erbil
Erbil, Iraq
¹m.kurd@hotmail.com, ²dr.laith@cihanuniversity.edu.iq, ³aram.m@cihanuniversity.edu.iq
DOI: 10.24086/cocos17.08

Abstract—Smartphones and wearable devices offer promising perspectives for processing and collecting velocity, variety, and high-quality data in healthcare scenarios. Collecting, investigating, analyzing, and mining health data to generate individual and public health rules. These rules will measure and enhance the quality of everyday life. However, current health systems are limited to their local data collection. As the current big data is so underutilized, there are many challenges, the aim of this study was to point these challenges to the big data technologies and big data.

Keywords-component: Big Data; Smartphones; Internet of Things, Machine learning; Healthcare.

I. INTRODUCTION

One of the most famous and biggest health systems is Kaiser Permanente, with more than nine million members, it manages data since 1945 almost a forty-four petabytes of Electronic Health Record (EHR) in that system alone. All the data entry has been entered by the hospital peripherals or operatives. Yet it’s not enough to generate health rules, distinguish between the good/bad life style, or to give notifications about the member health status outside the hospital.

Smartphone and wearable devices are the most carried devices by adults as well as kids, along with increasing number of sensors became the most vital dynamic source of information [9][12]. In 2015 there were 2.6 billion smartphone subscriptions in the world, the number of smartphone users is predicted to be 6.1 billion by 2020 [6]. The last decades have seen huge advance in the amount of routinely generated and collected data from sensors and applications are giving rise to a new research domain across most industries and is rightly considered the entrance to become more efficient and productive, along with the technologies to analyze and understand it.[2] Mobile Data volumes is growing faster than ever before, by 2020 near to 1.7 MB of information will be created every second for every human being on the planet..[5]

Data sets become complex or so large, can’t be easily stored or manipulate or analyze with traditional methods like spreadsheet, and R because of size, speed, format that encompassing the Big Data Three Vs: volume, velocity and variety [7].

II. CURRENT HEALTH CARE’S SYSTEMS

Most of the Health care systems contain electronic health record, which represents patient’s history, diagnoses and treatments, x-rays, computed tomography (CT) scan images, and magnetic resonance imaging (MRI) images. The current big data health system has limited advantages.
First, clinical value of Big-data revolution is being used to predict epidemics, cure disease, improve quality of life avoids preventable deaths, which most done in healthcare companies where they have patient’s information recorded structurally or nonstructurally in their computers, yet it is not efficient, accurate, with limited number life parameters, as these data are not dynamic and doesn’t explain current status, habits, behavior, and patient mental status.

Second, economical value, minimizing the cost by automated services, visualization, and reduce number of human factor in the system, yet insurance fraud still possible with missing of real human associated parameters.

Gain and analysis of patient-generated smartphone data provide solution for the current healthcare big data systems.

III. PRIVACY RULE

In 1996 Health Insurance Portability and Accountability Act (HIPAA) saw the light and activated in 1999. [3][4] A set of standards for the protection of certain health information. The main goal of this rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health. While this law written with absent of current smartphone services thus some of the smart phone or (IoT) devices collected data are protected by this law. At the same time such data are so sensitive it can’t be transferred, in addition, regarding other personal data, this is a challenge that most refuse to overcome. The reason that people don’t want to share their own “daily life Big Data” is more related to personal matters and sensitive data that they have.

Otherwise, if this line is crossed, for each user will provide more data that can be analyzed so that more accurate results can be obtained. With more detailed data, comes better results.

IV. PERSONAL DATA

Reading to the previous point, most of the new smartphones have at their hardware and software large amount of data that can generate and use it to server health system. Its available only of everyone shares it. [8]

For smartphone users, there is a difference between what is personal and public. The issue of what is personal and what is public mostly resides in the point of view of the services that they use. Statistically there is some of the persons don’t provide hospital or clinic on their actual data, convince persons to share their all their data with hospital or clinics still challenges in real life.

V. DIRTY DATA

Big data plays important role all over the world, but gaining those exclusive advantages requires having high quality data at the right time, that has become increasingly difficult to gain a clean data.

the value of big data for health decision-making purpose will be endangered if the data is not accurate or timely.

Often the data collected by hospitals’ input, mobile’s or Internet of Things (IoT)’s sensors, or user input are filled with mistakes, errors, incomplete values, duplicate data and incorrect data linking. This is referred to as dirty data.

The ability to transfer and store every piece of mobile data produces in its original form increase the problem. Dirty data costs time, processing and endanger the decision making. There are three possible ways to provide accurate big data are Cleaning and/or preventing.

First, batch processing through scripting after the data collection. Or interactively with data wrangling tools. both Data cleansing technologies consuming time; time is the second important factor in health systems, and it will lead to inaccurate decision by time.

Second, preventing dirty data by the proper preparations of establishing a structured, pattern collecting, sensor validation. That will lead to less inaccurate or false information on any forms it will transfer out. yet velocity of health Big data tends to be bursty, making it difficult to managed and predicted.

Moreover, Hybrid Health systems with data scrubbing, which is like data cleaning but more thorough, involving processes like filtering, validating, and translating. It possibly leads to consume time and processing over the decision has the same impact of standalone techniques.

VI. SHARED DATA

Scientists collaboration is most to promote the knowledge generating over the collected health big data. incase overcome all previous challenges of collecting every required clean data, still sharing these data consider as a big challenge [10]. So far no one figured out how share such dynamic big data, or specify the required data.

VII. TECHNIQUES

Big Data techniques starts with Mining, pattern recognition, natural language processing, visual analysis and all mathematical analytics and algorithmic based processing of data resources to generate descriptive, predictive and prescriptive models to analyze and derive insight from unstructured, semi-structured, and structured text data [11]
While The growth of the 3v’s of Smartphone data will continue to pose challenges with real-time techniques. It required techniques with ability to handle the different forms of the data all within reasonable time frames; such techniques of tools and services for generating integrated meaningful data with visualization are still required.

VIII. APPROPRIATE DATA
Collecting all smartphones’ sensing and data doesn’t necessarily lead to actionable insights, adding, the limitations of existing Data Analytics Architecture as only 10% of the ~ 2 petabytes of data is available for mining while 90% of ~2 petabytes of data are not opened nor analyzed properly resulting in premature data death. [14]

One of the data science challenges is to pinpoint a clear objective and the appropriate data sources to collect and analyze to meet up the objective, however. Once key patterns have been identified, Smartphone data collection must be prepared to act and make necessary changes in order to derive heath rule value from them.

IX. CONCLUSION
To adept smartphone data in healthcare system requires tuning the policies, infrastructure and technologies to meet such complexity and maintaining stewardship and privacy. These challenges go beyond the big data’s nature and features. One of the potential solutions is address some of these challenges at smartphone itself by generating timely filtered structured data entry to healthcare systems.

REFERENCES
[4] Diane Doebble Koch, JD, RN (2016) s the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?, health finance journal
Analysis of Confidentiality Algorithms in Different Mobile Generations

Khalid Fadhil Jasim  
Department of Computer Science, KICT  
International Islamic University Malaysia  
IIUM Cyber Security Malaysia Center for Cyber Space  
Security  
Kuala Lumpur, Malaysia  
khalid.jassim@yahoo.com

Imad Fakhri Al-Shaikhli  
Department of Computer Science, KICT  
International Islamic University Malaysia  
IIUM Cyber Security Malaysia Center for Cyber Space  
Security  
Kuala Lumpur, Malaysia  
imadf@iium.edu.my

DOI: 10.24086/cocos17.09

Abstract—In past years, a variety of Mobile technology generations have been adopted in mobile communication systems. Various sensitive information (e.g., emails, bank transactions, voice calls, ... ) was exchanged via the mobile systems. The protection of information confidentiality became a serious problem for the customers of these systems. Security solutions such as confidentiality cipher algorithms proposed to protect the transmissions in different mobile generations. The proposed cipher algorithms like A5/1 cipher, SNOW 3G cipher, ZUC cipher, and AES cipher were designed for securing mobile systems. This paper provides analysis study of operations and specifications for these cipher algorithms, and investigating the cryptanalysis methods which can be employed to attack these cipher algorithms.

Keywords- Mobile Generations; Cipher Algorithms; A5/1Cipher; SNOW3G Cipher; ZUC Cipher; AES Cipher; Cryptanalysis Attacks.

I. INTRODUCTION

In previous years, the researchers and industrials achieved massive advancement in Mobile communication and information technologies. Mobile technologies performed growing success and progress in different mobile generations. In this context, first generation systems (1G) appeared in (1980s), these analog systems presented voice calls without any protection. Shukla et al. [1] provided comparative study on various mobile generations, for instance, Mobile (1G) adopted cell signals with analog transmissions, offered expensive and less heavy devices. The standards in (1G) included Advanced Mobile Phone System (AMPS) and European Total Access Communication Systems (ETACS). The channel bandwidth was (30 KHz) in AMPS system. Some problems pointed out in Mobile (1G) such as low capacity, without security, and poor quality in voice calls. Second generation systems deployed in (1990s), these systems relied on digital communication, some standards like Global System for Mobile communication (GSM), and services supported by these systems included (emails, SMS messages, and digital faxes).

In Mobile (2G), Some important standards used like (CDMA, the Code Division Multiple Access technique) and (TDMA, the Time Division Multiple Access technique). The channel bandwidth in this generation was (30-200 KHz) and data rate transmission was (64 kbps) [2].

In (2000s), third generation with Universal Mobile Telecommunication System standards (3G-UMTS) was introduced. The (3G) systems adopted the technology of Mobile Broadband, delivered variety of mobile services (e.g. Internet with high speed access, multimedia applications, video conferencing via mobile nets, and digitized voice calls). Mobile (3G) presented features with enhancements (i.e. data transmissions with high speed, raised capacity of data and voice, supported packet data for networks). For example, Mobile (3G) with standards (CDMA2000, EV-DO) offered transmission data rate from (3.1 Mbp) to (14.7 Mbp), and the standards (HSPA, WCDMA) supported transmission rate from (14.4 Mbps) up to (63+ Mbps) [3].

Also, fourth generations systems was developed in (2010s) with faster broadband technology, based on some standards like Long Term Evolution technology (LTE). The (4G-LTE) systems presented some services for mobile networks customers, in which involved (Mobile Web Access, IP telephone services , Mobile TVs with HD technology, and Services of Cloud Computing). In mobile LTE technology the frequency bandwidth was (1.4-20 MHz), the peak of transmission rate reached (100 Mbps up to 326.4 Mbps) for downlink transmissions, and for uplink transmissions was (50 Mbps). Multiple antenna techniques (i.e. Beam forming, Spatial Division Multiple Access, and MIMO) have been used in Mobile LTE. Using of Multiple antenna techniques led to increase transmission rates, capacity of voice and data, and improved the efficiency in mobile (4G-LTE) systems [4].

In mobile technology there was a demand for high data transmission and new wireless mobile applications with enhanced features. Thus, researches have been started in fifth mobile (5G) generations and it is expected that (5G) will be adopted around (2020). In mobile (5G), the researches focused on improving worldwide wireless web (www), provide voice services via IP (VOIP), and Dynamic Adhoc Net (DAWN). The new features include data bandwidth (1Gbps and high), single unified standard, Multiple Access...
(CDMA and BDMA), core network (Internet), switching (All packet). Also, this generation provides broad band services (e.g. internet, voice, video streaming), and virtual private Net (VPN, Networks) is supported in (5G)[5,6].

Furthermore, stream ciphers and block ciphers algorithms have been proposed as confidentiality ciphers algorithms to ensure the security in different mobile communication systems. The A5/1 stream cipher algorithm was developed to protect users of mobile systems (2G-GSM) and prevent eavesdropping operations against these systems [7]. SNOW 3G is stream cipher algorithm represented the core confidentiality algorithm (UEA2), used as encryption algorithm in mobile phone systems (3G-UMTS). Design of SNOW 3G depends on register LFSR, Finite State Machine (FSM), and registers (R1, R2, and R3). Fault cryptanalysis can be used against SNOW 3G, in which the cryptanalyst may inject fault values in certain positions (Si) of LFSR during keystream generation mode. In this case, the cryptanalyst needs (22) fault values and (200) words of output keystream, then tries to extract values of keystream [8]. The stream cipher algorithm ZUC was designed to be adopted in confidentiality algorithm (EEA3-128), integrity algorithm (IEA3-128), and represented essential encryption in mobile systems (4G-LTE, Long Term Evolution mobile technology). Structure of ZUC relies on register LFSR, bit reorganization (BR), and non linear f-function. In initialization mode, ZUC cipher algorithm is loaded with values from IV key and secret key (K). In key stream operation mode the ZUC cipher produces words of key stream (Z). The key stream words used in encryption and decryption operation for packets of data in downlink and uplinks transmissions (i.e. in 4G-LTE devices) [9]. Additionally, AES cipher algorithm was block cipher algorithm and employed in mobile technology (4G-LTE). It was identified as (EEA2) confidentiality algorithm and (EIA2) integrity algorithm to achieve data confidentiality and integrity. The EEA2 algorithm was based on AES block cipher, in which it operates with 128-bit key and counter operation mode (AES-128 with CTR mode). During data encryption with block cipher algorithm (AES in CTR mode), the plaintext (PT) data divided into (128-bit) blocks, these blocks of (PT) are XORed with key stream blocks of AES cipher then produce blocks of encrypted data [10].

The paper organized as follows. Section II provides specification of A5/1 cipher algorithm and Guess and Determine cryptanalysis against this cipher algorithm. Description and operations of SNOW 3G cipher algorithm and Differential cryptanalysis attacks presented in section III. Section IV focuses on analysis components of ZUC cipher and Algebraic cryptanalysis attacks against this cipher. Versions of AES block ciphers, operations, descriptions, and Meet-in-the-Middle with biclique cryptanalysis for AES ciphers are presented in section V. Section VI provides analysis summery of confidentiality cipher algorithms and cryptanalysis techniques. Finally, some conclusions of this research are offered in last section VII.

II. A5/1 Cipher Algorithm

The A5/1 cipher algorithm was designed to protect the voice calls transmitted through GSM mobile communications. A5/1 was adopted as confidentiality algorithm in second generation mobile technology (2G-GSM) [11]. Also, A5/1 relied on stream cipher technique, the structure consists of (3) Linear Feedback Shift Registers (R1[19-bits], R2[22-bits], and R3[23-bits]). The secret key involves 64-bits (Kc with 64 bits). The feedback function of register R1 computed from positions (13, 16, 17, and 18), register R2 calculated from positions (20 and 21), and R3 from positions (7, 20, 21, and 22). The movement of three registers based on stop and go technique, so bit position (8) controls clock of R1, bit position (10) controls clock of R2, and position (10) controls R3. The 3 registers are clocked, then keystream (KS) is generated according to the following equation:

\[KS = R1[18] \oplus R2[21] \oplus R3[22]\]

(1)

Figure 1: A5/1 Cipher

The key stream generator is moved (224) steps and produce two blocks (BLOCK1 with 114-bits and BLOCK2 with 114-bits), represent the key stream (KS). The first part of key stream (BLOCK1) is adopted in the encryption of uplink transmission, the second part (BLOCK2) is used in decryption of downlink transmission (in Mobile Station Side). Moreover, BLOCK1 of key stream is used to decrypt uplink transmission and BLOCK2 to encrypt downlink transmission (in Network Side) [11].

Guess and Determine cryptanalysis attack may be used in cryptanalysis of A5/1 cipher algorithm. In 1994, Anderson[12] suggested this method to attack A5/1 algorithm, in which he proposed to guess the initial state (19-bits) of register R1, 22-bits of R2, and 11-bits of R3. The attacker will search \(2^{52}\), where \(19+22+11=52\) cases to determine the correct unknown bits of R3.

Cryptanalysis attack against this cipher was proposed by Golic [13]. In this attack, a system of linear equations were constructed then tried to solve the set of \(64 \times 64\) linear equations). The complexity of this attack was \(2^{52}\). First, half of initial values for registers (R1, R2, and R3) have been guessed, then the remaining initial values of these registers will be determined based on information extracted from known-keystream (KS, Equation 1).

Mahalanobis & Shah [14] presented an improved version of Guess and Determine cryptanalysis to attack A5/1 cipher. The average complexity of this attack method was required...
(2^{18.5}, search for possible cases). The attack is started by guessing (19-bits) of register R1, then the initial values of registers (R1 and R2) will be determined in next steps of the attack. It is assumed that (64-bits) of keystream are available for cryptanalyst. Also, the attack included Determination Phase and Post Processing Phase. In Determination Phase, the cryptanalyst tries to guess the values of (R1) and then identifies the values of (R1 and R2). Where, in Post Processing Phase, the A5/1 cipher is moved and produce outputs (i.e. stream of bits). The outputs are compared with the available (64-bits) of keystream, If the outputs matching with keystream then the initial values of registers (R1, R2, and R3) represent the values of secret key.

III. SNOW 3G Cipher Algorithm

The SNOW 3G cipher algorithm was developed by (ETSI/SAGE) and it was adopted as confidentiality cipher in third generation of mobile technology (3G-UMTS). This stream cipher algorithm depends on secret key (K with 128-bits) and Initial vector key (IV with 128-bits). The LFSR includes 16 stages (s_0, s_1, … s_15), finite state machine (FSM, with 3 registers R1, R2 and R3, each of 32-bit), and substitution boxes (S-boxes S1 and S2, each with 32-bit input and 32-bit output). The positions (s_5 and s_13) of LFSR are used as input to FSM to update the components of FSM (e.g. at clock t) as follows[15]:

\[
R_1^t = R_2^{t-1} \oplus (R_3^{t-1} \oplus s_5^{t-1}),
\]

\[
R_2^t = S_1(R_1^{t-1}), \quad R_3^t = S_2(R_2^{t-1}),
\]

\[
F^t = (s_{15}^{t} \oplus R_1^t) \oplus R_2^t.
\]

Where the symbol (\oplus) is addition modulo 2^{32} and (\oplus) is bit wise exclusive OR. Also, at the beginning of cipher algorithm operation, the LFSR initialized with values from IV key and secret key (K), the FSM is started with initial values (R1=R2=R3=0). The cipher algorithm runs (33 algorithm operation, the LFSR initialized with values from bit wise exclusive OR. Also, at the beginning of cipher algorithm operation, the LFSR initialized with values from IV key and secret key (K), the FSM is started with initial values (R1=R2=R3=0). The cipher algorithm runs (33 rounds from 33 rounds during initialization process of this cipher.

IV. ZUC Cipher Algorithm

The ZUC cipher algorithm is developed in china to be used as confidentiality and integrity algorithms (128-EEA3 and 128-EIA3 respectively) for the security of fourth generation mobile technology (Mobile 4G-LTE). The design of ZUC relied on three main parts: linear feedback register (LFSR), bit reorganization part, and the (f) as nonlinear function [17]. The initial input keys for this cipher involve initial vector key (IV with 128-bits) and secret key (K with 128-bits). The LFSR includes 16 stages (s_0, s_1, … s_15), where each stage s_i consists of 31-bits). The bit reorganization part consists of (32-bits) words (X0, X1, X2, and X3) and defined as follows:

\[
X0 = S_{13}H \| S_{13}L; \quad (\text{where } H \text{ is leftmost (16 bits) of word } S_{13} \text{ from LFSR and } \| \text{ is concatenation})
\]

\[
X1 = S_{11}L \| S_{11}H; \quad (\text{where } L \text{ is rightmost (16 bits) of word } S_{11} \text{ from LFSR})
\]

\[
X2 = S_{7}L \| S_{7}H;
\]

\[
X3 = S_{2}L \| S_{2}H.
\]

The words (X1 and X2) are employed as inputs to function (f), in which to update registers (R1 and R2). The remaining words (X0 and X3) adopted in computation of keystream (Z).

Moreover, the function (f) relies on two registers (R1 [32-bits], and R2 [32-bits]), two words (W1 and W2), and (32x32 bits) Substitution box S (S-box S):

\[
W = (X0 \oplus R1) \oplus R2; \quad (\oplus \text{ is exclusive OR, } \oplus \text{ is addition mod 232})
\]

\[
W1 = R1 \oplus X1; \quad W2 = R2 \oplus X2;
\]

\[
R1=S-Box(S(L1 \| W1L \| W2H); \quad (\text{where } L \text{ is rightmost (16 bits) of word } W1)
\]

\[
R2=S-Box(S(L2 \| W2L \| W1H)); \quad (\text{where } H \text{ is leftmost (16 bits) of word } W1)
\]

The linear transformations L1 and L2, used in function (f), is computed as shown:

\[
L1(X)=X \oplus (X \ll 2) \oplus (X \ll 10) \oplus (X \ll 18) \oplus (X \ll 24),
\]

\[
L2(X)=X \oplus (X \ll 8) \oplus (X \ll 14) \oplus (X \ll 22) \oplus (X \ll 30). \quad (\text{where } X \ll n \text{ is the n-bit cyclic shift of 32-bit word } X \text{ to the left}).
\]

Differential cryptanalysis attacks can be used to analyze SNOW 3G cipher [16]. In this method, it is noticed that if there is no feedback from (FSM) to (LFSR), during initialization operations (clock No.1 to clock No. 32), and the cryptanalyst gained information about pair of (IV keys). Then this cipher algorithm can be attacked and crypt analyzed by using differential method (with known IV), the required complexities of this attack are (2^{32}) for the time and (2^{57}) for data of keystream. In case there is a feedback (from FSM to LFSR), the same attack's method can be adopted in cryptanalysis of 16 rounds from 33 rounds during initialization process of this cipher.
During the keystream generation mode, ZUC cipher algorithm produces (32-bits) word of keystream \((Z_t, \text{at clock } t)\) as follows:

\[
Z_t = (X_0 \oplus P_0^t) + p_2^t \oplus X_3^t
\]  
(3)

The sequence of keystream words are adopted in encryption and decryption processes for transmitted data via mobile communications.

Figure 3: ZUC Cipher

Algebraic cryptanalysis method may be adopted to attack ZUC cipher. In this attack, the cryptanalyst tries to find indirect relation between bits sequence of keystream \((Z)\) and internal state of this cipher algorithm. It will be considered that the non linear filter function as combiner function. The inputs to combiner function include four words \((X_0, X_1, X_2, \text{and } X_3)\) extracted from LFSR, and the output is 32-bits word of keystream \((Z\) with 32-bits). To establish a relation between the four inputs and the one output, a matrix is constructed, in which to simulate the combiner. Matrix columns involve monomials \((128\text{-bits of four inputs and } 32\text{-bits of outputs } Z \text{ to combiner function})\), and Matrix rows include four input words \((X_0, X_1, X_2, \text{and } X_3)\). This method of attack can be used to solve the system of equations and extract secret key (initial state of LFSR) of ZUC cipher with keystream data \((2^{297})\) and complexity of needed operations \((2^{282})\) [18,19].

These two algorithms represented the second set of algorithms in fourth generation of Long Term Evolution in mobile systems technology (Mobile 4G-LTE technology)[20].

In AES-128 bit, the main encryption and decryption operations are applied on state array with size \((4\times4\text{ bytes as }2\text{ dimension matrix})\). The input plaintext \((128\text{-bits}),\) is represented as 16 bytes, and arranged in state array \((4\times4\text{ bytes})\). Each round of AES-128 (10 rounds in AES-128) adopts four mathematical operations on state array:

1. **Sub Bytes Operation (SB):** represents nonlinear mathematical transformation, in which it applies the substitution box (S-Box) on all the 16 (bytes), which already exist in state array \((4\times4\text{ matrix of input plain bytes})\).

2. **Shift Rows Operation (SR):** denotes linear mathematical transformation, the target of this operation is to rotate the row number \((i, \text{ith row})\) of state array by value \((i\text{-bytes})\) to left direction, \((i=0,1,2,3)\).

3. **Mix Columns Operation (MC):** also, this operation represented linear mathematical transformation, in which each column of state array is multiplied by constant array \((4\times4\text{ matrix of constant bytes})\) and the math operations defined in the field \((GF(2^8))\).

4. **Add Round Key Operation:** the AES-128 bit depends on 10 rounds, therefore the 16 bytes of state array, in round number \((i)\), are XORED with 16 bytes of related round key \((R_{Ki})\). Furthermore, The AES-128 cipher relies on secret key with \((128\text{-bits}),\) and key schedule procedure used to produce \((11\text{ round sub keys (Round Key-0, Round Key-1, \ldots, Round Key-10})\). First round key is extracted from secret key bytes, then each of remaining round keys \((R_{Ki}, \text{where } i=1,2, \ldots, 10)\) produced depending on its predecessors sub round keys \((R_{Ki-1})\).

In addition, Meet-in-the-Middle cryptanalysis is a technique which can be employed to attack block ciphers [21]. Biclique cryptanalysis technique proposed to attack hash functions family (SHA-2 family, Skein-512 hash function). Also, Biclique technique can be adopted to attack different versions of AES block cipher. The idea of Biclique cryptanalysis against AES cipher is based on the Biclique concept presented in [22].

In Biclique cryptanalysis, first the function \((f)\) is defined as function that transforms internal state \((S)\) of block cipher to output ciphertext \((C)\):

\[
f_K(S) = C
\]  
(4)

Here, function \(f\) is connected the input \((2^d)\) of internal states \((S_i),\) \((2^d)\) ciphertext \((C_i),\) and \((2^d)\) cipher keys \((K[i,j])\). Thus, Biclique with \((d\text{-dimension})\) is defined by three elements, \([(C_i), \{S_i\}, \{K[i,j]\}]\):

\[
C_i = f_{K[i,j]}(S_j) \text{ for all } i,j \in \{0, \ldots, 2^d - 1\}
\]  
(5)
In this cryptanalysis attack, Biqileic attack can be performed according to the following steps:

- The cryptanalyst tries to partition the space of cipher key (K) for groups (K[i,j], matrix with $2^d \times 2^d$ dimensions), and Encryption of block cipher (E) is assumed as two sub ciphers ($E=f \circ g$).
- The cryptanalyst creates structure which includes possible ciphertexts ($2^d$ of C), intermediate possible states ($2^d$ of $S_i$), and such that decipherment of ciphertext ($C_i$) leads to the state ($S_i$) of the block cipher.
- The cryptanalyst performs the decryption operations on possible ciphertexts ($C_i$), based on secret cipher keys (K[secret]), then producing the possible plaintexts ($2^d$ of $P_i$).
  \[ C_i \xrightarrow{\text{decryption oracle}} P_i \]
- The Secret key (K[secret]) is identified, when it leads to transform state ($S_i$) to plaintext ($P_i$), and it is one of the cipher keys ($K[i,j]$) under tests.
  \[ \exists i, j : P_i \xrightarrow{K[i,j]} S_j \]

As a results, to recover the key of AES-128 bit (for 8-round from 10), the requirements involved complexity of memory with ($2^d$), complexity of data is ($2^{88}$), and complexity of computations ($2^{57.34}$). The requirements for AES-192 bit (9-round from 12) included complexity of memory with ($2^d$), complexity of data is ($2^{80}$), and complexity of computations ($2^{282}$). With respect to AES-256 bit (9-round from 14), the complexity of memory was ($2^d$), complexity of data was ($2^{32}b$), and complexity of computations ($2^{59.81}$) [23].

VI. DISCUSSION

The analysis summary of Cipher algorithms and cryptanalysis techniques (shown in TABLE 1 and TABLE 2) are follows:

- The cipher algorithms (A5/1, SNOW 3G, and ZUC) are adopted design of stream ciphers, where AES relied on design of block ciphers.
- The structure of A5/1 algorithm was simple, consists of 3 LFSRs and function with (XORs operations).
- The structures of SNOW 3G and ZUC Ciphers were more complicated adopted different components (e.g. LFSR [16 words], FSM, memory registers Rs, Non linear functions, and S-boxes), in which enhanced the security for these ciphers.

- The structure of AES relied on three versions (AES-128 with 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds). Each round depends on Sub Bytes, Shift Row, Mix Column, and Add Round Key operations, S-boxes as well. Different number of rounds, the four operations, variety of keys (128-bits, 192-bits, and 256-bits), were made AES block cipher with better security over three mentioned stream ciphers.
- Moreover, A5/1 cipher used to secure (2G-GSM) Mobile systems, SNOW 3G for security of (3G-UMTS) Mobile systems, ZUC and AES ciphers in (4G-LTE) Mobile systems.
- Various Cryptanalysis techniques can be used to attack these cipher algorithms. Guess and Determine adopted to attack A5/1 cipher. The cryptanalyst targets to guess (19 bits) of register R1, using (64-bits) of keystream, and tries to identify values of registers R2 and R3. This attack requires, complexity computations ($2^{48.5}$), data complexity ($2^8$). To attack initial key with brute force it is required complexity computations ($2^{64}$).
- Differential cryptanalysis used to attack SNOW 3G cipher. The IV key (128-bit) used in SNOW 3G during encryption operations, and it is transmitted via communication channels. Thus, the cryptanalyst can use differential method with known information of IV keys, focused on pairs of IVs and steps of keystream generation (clock-1 to clock-32). This type of cryptanalysis against SNOW 3G, needs complexity computation ($2^{57}$), and data complexity ($2^{31}$) for the keystream. Also, the secret key K with (128-bit) in this cipher, and the required complexity is ($2^{128}$) for brute force attack.
- Algebraic cryptanalysis can be applied to attack ZUC cipher. In this method, the nonlinear function treated as combiner function. Four (32-bit) words (X0, X1, X2, and X3) are taken from register LFSR, used as inputs to combiner function, then (32-bit) keystream (Z) represents output of this combiner function. Matrix is created based on (128-bits) of the four inputs and (32-bits) of (Z) keystream. Thus, the cryptanalyst tries to solve system of equations, then reveals values of secret key K (i.e. 128 bits used to initialize register LFSR). To perform this attack, the needed data complexity is ($2^{97}$) for keystream, and computations complexity is ($2^{282}$). Brute force attack required ($2^{128}$) computation complexity based on (128-bits) of secret key.
- Meet-in-the-Middle with Biqileic techniques used to attack (3) versions AES cipher. These attacks depend on sequence of steps. First, the space of secret ciphering key divided to groups and treated...
as matrix (K[i,j], with $2^d \times 2^d$ dimensions), block cipher encryption (E) with two sub ciphers (f and g). Next, establish structure involves possible ciphertexts ($2^d$ of C), possible states ($2^d$ of S), based on group of keys, decryption of ciphertext to produce state (S). Then, decryption applied on possible ciphertexts (C), using secret keys (Ksecret), and generating possible plaintexts ($2^d$ of P). For instance in AES-128, the data complexity is ($2^{128}$), and complexity of computations ($2^{125.34}$). But in AES-256, the data complexity is ($2^{192}$), and complexity of computations ($2^{251.92}$).

<table>
<thead>
<tr>
<th>Cipher Algorithms</th>
<th>Type of Cipher Design</th>
<th>Components of Cipher Algorithm</th>
<th>Encryption/Decryption Keys</th>
<th>Mobile Generations</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES/1</td>
<td>Stream Cipher</td>
<td>-LSFR[118-bits], LFSR[2-bit]</td>
<td>-R(64-bits), -IV(128-bits)</td>
<td>Mobile(3G-GSM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Function(with 2 XORs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-FSM, R1[32-bits], R2[32-bits], S-Boxes(S1, S2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Bit Reorganization(X0, X1, X2, X3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Non linear Function, R1[32-bits], R2[32-bits], S-Boxes(S0, S1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>Block Cipher</td>
<td>-State array (4x4 bytes)</td>
<td>-R(128-bits), -IV(128-bits)</td>
<td>Mobile(4G-LTE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Sub Byte Operation (SB), Shift Row Operation (SR), Mix Column Operation (MC), Add Round Key Operation (ARK)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 1: CIPHER ALGORITHMS AND MOBILE GENERATIONS**

<table>
<thead>
<tr>
<th>Cipher Algorithms</th>
<th>Type of Cryptanalysis Attack</th>
<th>Computations Complexity Of Attack</th>
<th>Data Complexity Of Attack</th>
<th>Complexity Of Brute Force Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES/1</td>
<td>Guess and Determine Cryptanalysis</td>
<td>$2^{45.5}$</td>
<td>$2^6$</td>
<td>$2^{64}$</td>
</tr>
<tr>
<td>SNOW 3G</td>
<td>Differential Cryptanalysis</td>
<td>$2^{57}$</td>
<td>$2^{33}$</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td>ZUC</td>
<td>Algebraic Cryptanalysis</td>
<td>$2^{202}$</td>
<td>$2^{27}$</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td>AES</td>
<td>Biologic Cryptanalysis, Based on Meet-in-the-Middle Attack</td>
<td>-AES-128, $2^{125.34}$, -AES-192, $2^{192}$, -AES-256, $2^{251.92}$</td>
<td>-AES-128, $2^{58}$, -AES-192, $2^{96}$, -AES-256, $2^{128}$</td>
<td>-AES-128, $2^{128}$, -AES-192, $2^{192}$, -AES-256, $2^{224}$</td>
</tr>
</tbody>
</table>
VII. CONCLUSION

This paper introduced analysis study of confidentiality cipher algorithms in different mobile technology generations. First generation (Mobile 1-G) was without protection. Second generation (2G-GSM) relied on A5/1 cipher algorithm. A5/1 cipher possessed simple design (3 LFSRs, XORs operations) and offered weak protection. Third generation (3G-UMTS) adopted SNOW 3G cipher for data protection and authenticity. SNOW 3G involved rigid design, more secure, with various components (LFSRs, FSM, Registers, and S-boxes). Fourth generation (4G-LTE) employed ZUC and AES ciphers for integrity and confidentiality algorithms. ZUC cipher included secure design, based on different components (LFSRs, Bit Reorganization, non linear functions, Registers, and S-boxes). AES cipher was with 3 versions (AES-128 with 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds). In AES ciphers, the rounds relied on different mathematical transformations (Sub Bytes, Shift Row, Mix Column, Add Round Key operations, and S-boxes). In addition, there was research progress efforts on fifth mobile generations (5G), it is still under research, the researches focused on improving worldwide wireless web, and enhance wireless mobile features, it is expected that (5G) will be presented around (2020).

Finally, this paper investigated some cryptanalysis techniques (Guess and Determine for A5/1 cipher, Differential cryptanalysis for SNOW 3G cipher, Algebraic cryptanalysis for ZUC cipher, and Meet-in-the-Middle with Biclique techniques for 3 versions of AES cipher).

REFERENCES


Comprehensive Study of Hierarchical Routing Protocols in MANET using Simple Clustering

Ghassan A. QasMarrogy  
Communication and Computer Engineering Department  
College of Engineering, Cihan University, Erbil  
Erbil, Iraq  
Ghassan.qasmarrogy@cihanuniversity.edu.iq

Husham J. A. Alqaysi  
Communication and Computer Engineering Department  
College of Engineering, Cihan University, Erbil  
Erbil, Iraq  
dr.hisham.j@cihanuniversity.edu.iq

Yazen S. Almashhadani  
Communication and Computer Engineering Department  
College of Engineering, Cihan University, Erbil  
Erbil, Iraq  
yazan.saif@cihanuniversity.edu.iq

DOI: 10.24086/cocos17.10

Abstract—The rapid evaluation of data transmission in wireless communication technologies can show many problems. In the previous year’s many routing protocols was developed, implemented, and evaluated for transmission of data in the Mobile ad hoc network (MANET), where it envisioned to be a useful technology in military communication systems and other areas. One of the routing protocols used in MANET is the hierarchical routing protocol that considered an energy efficient. Therefore, in this paper, a comprehensive study will be presented of the hierarchical routing protocol for MANET in order to expose new open issues to either improve the existing routing techniques or to develop new routing solutions for other researchers. The reviewed routing protocol is designed to support networks of a medium size, containing approximately between 150 to 250 nodes but less than 3,000 nodes. The reviewed design is intentionally simple to allow ease of implementation in comparison with other MANET protocols that provide similar functionality.

Keywords- MANET, proactive routing, reactive routing, hybrid routing, clustering, Hierarchical routing.

I. INTRODUCTION

A computer network can be categorized as wired or wireless [1]. Where wireless can be distinguished from wired with their physical connectivity links between the nodes are not needed [2]. Data routing is an activity or a function that transmit a message from the source to destination in telecommunication networks and also play an important role in architecture, design, and operation of networks [3]. Ad-hoc networks are wireless networks where each node communicate and transmit with each other using multi-hop links. There is no fixed infrastructure or Access point (AP) for communication [4]. Each node itself acts as a router for forwarding and receiving packets between other nodes. The Routing process in ad-networks has been a challenging task ever since the wireless networks came into existence [5]. The key reason for this is the endless change in topology of the network, due to of its high degree of node mobility, therefore a number of protocols have been developed for accomplishing this task. Wireless communication is established by nodes acting as routers and transferring packets from one to another, were it called Mobile ad-hoc networks (MANET). Routing in these networks is highly complex due to moving nodes and hence many protocols have been developed. In this paper, a hierarchical algorithm for routing in a mobile ad hoc network (MANET) was studies and reviewed. This algorithm provides the ability to grow from small to big networks through the use of clustering. The algorithm does not provide routing, but rather allows for the use of different routing protocols on top of the clustering protocol.

To summarize, this paper was organized in 5 sections, section 2 deals with an introduction to MANETs routing protocols, section 3 will explain the proposed routing algorithm and clustering creation, while section 4 will show a detailed explanation of the hierarchical routing protocol and how its work. And finally, section 5 is the discussion, conclusion and the future work of the paper.

II. MANET ROUTING PROTOCOLS

One of the biggest problems in MANET design is how to guide the Routing packets to the destination node. If the routing of packets fails to be delivered which is the equivalent of failure of the MANET network, even if the nodes in MANET continue to function. MANET routing is based upon a variety of algorithms and currently, MANET routing uses three basic approaches to route packets. One approach is a proactive protocol where each MANET node maintains a local copy of a full routing table for the MANET. Another approach is to use a reactive protocol where each route is built on demand and only maintained while data is actively traveling the route. A third approach is a hybrid protocol that combines both proactive and reactive behavior. This combination generally involves
partitioning the network into small areas. The behavior of the routing is based on the location of the source node and the destination node. The routing of a packet inside of one of the networks areas is done via a proactive routing protocol. When the packet must cross between areas of the network a reactive routing protocol is used [6]. Figure one shows the types of routing protocols.

Regardless of the routing protocol that is chosen for a MANET, improvements are available. These improvements further enhance the performance of routing in the MANET. Usually, these improvements involve "link break" scenarios where two nodes will be separated. Security may be added in the form of enhancements to existing protocols, other times security is the basis for the protocol and drives the implementation. Security in ad hoc routing is based on three principles: Availability, Confidentiality, and Integrity [7]. There are many enhancement presented where it may be implemented side by side to enhance a single existing protocol, such as Encounter Age Caching, Non-Optimal Route Suppression, Bloom Filter Service Discovery, Abstraction of Bidirectional Routes, Route Caching Chase Packets, Route Compaction, Swarm Intelligence, Localized Error Recovery, Global Positioning System (GPS) Enabled Nodes.

As the number of nodes in a MANET grows, the ability to route inside of that MANET is decreased. For proactive protocols, this is because each node attempts to maintain routing information for every node in the MANET. This is difficult due to the memory requirements and due to the control requirements. The number of control packets will increase quadratic ally based on the number of nodes in the MANET. As for reactive protocols, they do not maintain the entire network state at the node level, the individual nodes generally do not have problems, for instance, due to memory constraints. Hybrid protocols suffer in both ways due to the combination of routing protocols. A hybrid protocol operates with more nodes than either a pure proactive or pure reactive routing protocol but still does not scale well. As the proliferation of devices continues, the potential size of a MANET will continue to increase and a new solution must be obtained. Therefore by studying the developed clustering algorithm that will be independent of the underlying MANET routing protocol to understand solving the above problem. The protocol will use an approach similar to ZRP [8], where the routing inside of a cluster uses a different protocol from the routing between clusters. Ideally, the clustering protocol may be implemented without requiring modifications to any routing protocol that wished to use clustering, and this algorithm accomplishes that.

Figure 2.1: types of routing protocols.

The clustering will be done by adding fields to the packet header to indicate different types of packets, such as a cluster control packet or a packet relating to the underlying routing protocol. Further nodes will be modified so that they know the current cluster head, the backup cluster head and maintain several routing tables.

III. CLUSTER CREATION AND MAINTENANCE PROTOCOL

The major key of this paper is the cluster creation and maintenance protocol, where it shows a different way of looking at clustering inside of a MANET. The protocol is divided into different sections including the bootstrapping of the protocol, how a node joins a cluster, how a node determines that there is a link break from the "cluster masters", the procedure a node follows once a disconnect has been detected, and finally, how routing is accomplished, both intra-cluster and inter-cluster. The cluster masters are the cluster head node and the backup cluster head node

A. Assumptions for Cluster Nodes

There are some assumptions for the cluster nodes. The first assumption is that each node has a unique identifier that is generated from some internal information such as a hash of the nodes primary processor identifier and the MAC address from the primary interface of the node. The protocol also assumes a maximum number of nodes that are in a cluster to be a fixed number of nodes. The protocol has a default soft limit of 50 nodes to a cluster and a hard limit of 75 nodes.

B. Bootstrapping the Protocol

When a node first booting, the node is not a member of any cluster. It will create a new cluster and be the head of that cluster. Figure 3.1 gives an example network with 13 nodes labeled A through M.
C. Cluster Formation

At the beginning, no clusters have been formed and each node is a cluster head in a cluster with a total node count of one. Each node will broadcast an initial Cluster Hello packet (CH). This packet is the basis for determining both the nodes in the cluster and the links between the clusters. Upon receiving a CH packet the node will generate a Cluster Hello Reply packet (CHR) based on whether or not the node is a member of the cluster. If the node is a member of the cluster, then the node will re-broadcast the CH packet and will wait a specified amount of time before formulating a CH packet. If the node is not a member of the cluster, then the node will not send a CHR packet. Since the clusters all contain a single node, each node will receive a CH packet from different clusters. Each node will then realize that no other nodes in the neighborhood are a part of the cluster. This is because no neighbor of the node is in the nodes cluster.

The node will then send out a Cluster Merge Request packet (CMP). The CMP packet is sent to a cluster gateway and is always forwarded up to the cluster head in the receiving cluster. The receiving cluster head then must make the decision of whether or not to merge with the requesting cluster. If the decision to merge is reached, then the receiving cluster head will send out a Cluster Merge Preapproval packet (CMP) back to the original cluster.

Upon receiving a CMP packet the requesting cluster head must now decide to merge or not to merge. If the requesting cluster head decides to merge, then a Cluster Merge Approved packet (CMA) is sent. At this point, if requesting cluster head will either be the new cluster head of the merged cluster or will become the new backup cluster head for the merged cluster. If the requesting cluster head will remain the cluster head, then a Cluster Head Backup packet (CHB) will be sent out to the cluster, otherwise, the requesting cluster head will become the backup cluster head and will send out a Cluster Hand Takeover packet (CHT). The CHB instructs all current members of the cluster to reset the backup cluster head to be the backup cluster head indicated in the CHB packet. The CHT instructs all nodes to set the backup cluster head to be the current cluster head and to set the cluster head as the cluster head node that originated the CHT packet.

D. Cluster Maintenance

Cluster maintenance is performed by the periodic broadcasting of the CH packets and the reception of the CHR packets. The CH packets prove to the cluster nodes that the cluster head is still reachable, provide the latest snapshot from the cluster head of all nodes that are currently in the cluster, and gives the identifier of the backup cluster head. Upon receipt of a CH packet, the current node will update the intra-cluster routing table by either reconciling with the node list in the CH packet or completely rebuilding the table based on the node list in the CH packet. The current node will now generate a CHR packet that contains the identifier of the current node as a cluster member, and a list of all cluster gateway nodes from the current nodes neighborhood table. This will allow the cluster head to have a routing table that contains information on how to reach each neighboring cluster. The current node will now re-broadcast the CH packet to all nodes in the neighborhood. Upon receipt of a duplicate CH packet, the current node will simply drop the packet. The current node tells if a packet is a duplicate because of a sequence number contained in the CH packet. If the current node does not receive a CH packet from the cluster head, and further did not receive a CHT packet from the backup cluster head, then the current node will assume that due to network changes the current node has become isolated from the cluster. In this case, the current node will reset, as though initially bootstrapping the protocol, and will become the cluster head and backup cluster head of a cluster that contains one node, the current node. Figure 3.2 show how source node contact the CH nodes for transmitting the packets of data.
B. Maintained Data

Every node in the cluster is responsible for maintaining a certain amount of data. This data is what allows the nodes to make decisions about how to perform routing both within the cluster and between other clusters. Depending upon the roles of the node some of the data may not need to be maintained.

C. Packet Handling

The processing of different types of received packets is the basis for the Simple Cluster Protocol. These packets each provide a piece of the functionality required for this protocol. Only the Lower Level Routing packet contains data to be routed between nodes in the MANET. The Cluster Hello packet (CH) is the beacon that maintains the cluster. This packet is sent out periodically by the Cluster Head, it contains a snapshot of all nodes in the cluster given by the cluster head. Then a Cluster Hello Reply packet (CHR) is generated by a node n when n receives a CH packet from a node in the same cluster as n. The CHR packet for each node is propagated back to the cluster head for that nodes cluster. Only the cluster head and the backup cluster head will process a CHR packet. The processing for a CHR packet involves maintenance of two items: the list of nodes in the cluster and the gateway links from the node that generated the CHR packet. To merge two clusters to become one a Cluster Merge Request (CMR) packet is generated. Only the cluster head will process the CMR packet. All other nodes in the cluster will relay a CMR packet to the cluster head. The cluster head will process the merge request. After that, a Cluster Merge Preapproval (CMP) packet will indicate that the target merge cluster has agreed to merge with the cluster that sent the initial merge request packet. Finally, a Cluster Merge Approval Packet will be sent from the target cluster, destructive changes have already been done, and this packet allows the requesting cluster to finalize the merge and perform post merge clean up, as required. In the end, a Cluster Head Takeover Packet is generated and signifies that a new cluster head is taking control. This phenomenon happens under two conditions; the backup cluster head determines the cluster head has failed or two clusters merge, whereby one of the clusters will have a new cluster head. Two more packets also will be generated, the Cluster Head Backup Takeover (CHBT) packet which will be applied to the cluster head backup. And the Cluster Sync (CS) packet, which is used to synchronize the information contained in the cluster head with the backup cluster head.

V. CONCLUSIONS AND FUTURE WORK

Many areas of research remain incomplete regarding the presented cluster protocol. This paper presented a study for the hierarchical cluster MANET routing protocol that allows for mid-range scaling of the number of nodes in a MANET. By providing a clustered approach that does not directly specify the underlying routing protocols, more flexibility is given in the deployment of the MANET. The underlying routing protocols can be chosen suit the specific MANET situation. This protocol was specified with a detailed example of cluster organization. Additionally, this paper gives a brief background of different areas in MANET routing protocol such as proactive, reactive and hybrid. As a conclusion, the clustering is not suited to all possible MANET situations and is detrimental if the size of the MANET is small. If the MANET contains less than 200 nodes the overhead of the clustering protocol will cause the routing in the MANET to be less efficient. This algorithm is postulated to be effective once the number of nodes exceeds 200, depending upon the size of the clusters. This is due to the increased efficiency of determining a route due to the reduction of flooding in the network. One future goal would be to extend the clustering implementation from a single level of clustering to provide N levels of clustering. Future work should include simulations that compare this protocol to other clustering protocols. These simulations can also verify the breakeven point of the algorithm under various MANET scenarios. An avenue to be explored involves the use of location information to help clusters avoid forming when the links that join the clusters are estimated to be short lasting.

REFERENCES

Performance Analysis of OFDM with Different Cyclic Prefix Length

Yazen S. Almashhadani
Communication and Computer Engineering Department
College of Engineering, Cihan University
Erbil, Iraq
Yazan.saif@cihanuniversity.edu.iq

Husham J. A. Alqaysi
Communication and Computer Engineering Department
College of Engineering, Cihan University
Erbil, Iraq
dr.hisham.j@cihanuniversity.edu.iq

Ghassan A. QasMarrogy
Communication and Computer Engineering Department
College of Engineering, Cihan University
Erbil, Iraq
Ghassan.qasmarrogy@cihanuniversity.edu.iq

DOI: 10.24086/cocos17.12

Abstract— Due to the spectacular growth of the wireless services and demands in recent years, Orthogonal Frequency Division Multiplexing (OFDM) is a latest and suitable modulation scheme for commercial high-speed broadband wireless communication systems. OFDM is one of the main techniques proposed to be employed in 4th Generation Wireless Systems. One of the OFDM key parameters is a cyclic Prefix (CP). Cyclic prefix is a guard time length padded with every OFDM symbol to completely alleviate Inter-symbol Interference (ISI) and to preserve orthogonality among OFDM subcarriers as long as the guard time length is sufficiently greater than channel delay spread. This paper analyzes OFDM system and the effect of cyclic prefix and length of cyclic prefix on OFDM system. Besides, compare the performance of the system with and without cyclic prefix. The simulations were carried out over AWGN and Rayleigh fading channels, and the results have been compared with the theoretical ones.

Keywords- OFDM; BER, BPSK; Cyclic prefix; ISI

I. INTRODUCTION

In Orthogonal Frequency-Division Multiplexing (OFDM) scheme a large number of narrow band sub channels are used to transmit high data rate. These sub channels are orthogonal to each other. They are closely spaced and narrow band. OFDM is being used because of its capability to handle with multipath interference at the receiver. The main principle of OFDM is to split a high rate data stream into a number of lower rate streams that are transmitted simultaneously over a number of subcarriers. The relative amount of dispersion in time caused by multipath delay spread is decreased because the symbol duration increases for lower rate parallel subcarriers. As modulation scheme can be used basically any form of digital modulation, the most common being BPSK, QPSK and QAM. The outputs of all the modulators added and the result is the signal to be transmitted. The OFDM system using channel coding and BPSK modulation produce minimum value of BER as compared to other modulation technique. So BPSK based OFDM system using FFT and cyclic code produces minimum value of BER [1].

The basic idea of OFDM is to divide the available spectrum into several orthogonal sub channels so that each narrowband sub channels experiences almost flat fading. The major advantages of OFDM are its ability to convert a frequency selective fading channel into several nearly flat fading channels and high spectral efficiency. The orthogonality of the carriers means that each carrier has an integer number of cycles over a symbol period. This implying the spectrum of each carrier has a null at the center frequency of another carriers in the system. This results in no interference between the carriers, allowing then to be spaced as close as theoretically possible. This overcomes the problem of overhead carrier spacing required in FDMA. Each carrier in an OFDM signal has a very narrow bandwidth (i.e.1kHz), thus the resulting symbol rate is low. This results in the signal having a high tolerance to multipath delay spread, as the delay spread must be very long to cause significant inter-symbol interference (e.g. > 500 µsec) [2].

The level of robustness can in fact be increased even more by the addition of a guard period between transmitted symbols. The guard period allows time for multipath signals from the previous symbol to impair before the information from the current symbol is gathered. The most effective guard period to use is a cyclic extension of the symbol [3].

II. OFDM TRANSCEIVER

The basic model of OFDM system is shown in Fig. 1. That is, the transmitter section modulate a digital data to be transmitted using BPSK modulation technique then the data is converted to several parallel stream. The modulated signals are
processed by IFFT block to transform the spectral representation of the data into the time domain as it is much more computationally efficient, and so is used in all practical systems [4, 5]. Then the cyclic prefix is added to the signals. The cyclic prefix, which is transmitted during the guard interval, consists of the end of the OFDM symbol copied into the guard interval, and the guard interval is transmitted followed by the OFDM symbol. The reason that the guard interval consists of a copy of the end of the OFDM symbol is so that the receiver will integrate over an integer number of sinusoid cycles for each of the multi-paths when it performs OFDM demodulation with the FFT. OFDM has excellent robustness in multi-path environments. Cyclic prefix preserves orthogonality between sub carriers. Cyclic prefix allows the receiver to capture multipath energy more efficiently. Then the signals are converted to serial form and transmitted through transmitter. Digital data is then transmitted over the channel.

At the receiver the reverse process is performed. The serial data is received which is converted to parallel form. Then cyclic prefix is removed. After removal of cyclic prefix, Fast Fourier Transform is performed. Then the signals are demodulated to get the original data.

### III. OFDM SYMBOLS WITH CYCLIC PREFIX

Cyclic prefix is a guard interval in time domain which inserts between OFDM symbols to mitigate the inter-symbol interference (ISI). Cyclic Prefix is to extend the OFDM symbol by copying the last segment of the OFDM symbol into its head side. Let $T_G$ and $T_{sym}$ denote the length of CP in terms of samples and symbol duration. Therefore the extended OFDM symbols now have the duration of $T_{sym(G)} = T_{sym} + T_G$. Fig. 2 shows two consecutive OFDM symbols, each of which has the CP of length $T_G$. Fig. 3 illustrates them jointly in the time and frequency domains. Fig. 4 shows the ISI effects of a multipath channel on some subcarriers of the OFDM symbol. It can be seen from this figure that if the length of the guard interval (CP) is set longer than or equal to the maximum delay of a multipath channel, the ISI effect of an OFDM symbol (plotted in a dotted line) on the next symbol is coned within the guard interval so that it may not affect the FFT of the next OFDM symbol, taken for the duration of $T_{sym(G)}$. Guard interval should be longer than maximum delay of the multipath channel for maintaining the orthogonality among the subcarriers [6]. As the continuity of each delayed subcarrier has been warranted by the CP, its orthogonality with all of the subcarriers is maintained over $T_{sub}$ [7].

![Basic OFDM Transceiver](image)

**Figure 1.** Basic OFDM Transceiver

![OFDM Symbol with Cyclic prefix](image)

**Figure 2.** OFDM Symbol with Cyclic prefix

![Time/Frequency domain OFDM Symbol with CP](image)

**Figure 3.** Time/Frequency domain OFDM Symbol with CP

![ISI effect on OFDM Symbol](image)

**Figure 4.** ISI effect on OFDM Symbol

### IV. RAYLEIGH MULTIPATH CHANNEL MODEL

Rayleigh fading channel model, is a statistical model which is reasonable for an environment where there are large numbers of reflectors. The channel is modelled as n-tap channels with each the real and imaginary part of each tap being an independent Gaussian random variable. The impulse response is,

$$h(t) = \frac{1}{\sqrt{n}}[h_1(t-t_1) + h_2(t-t_2) + \ldots + h_n(t-t_n)]$$

(1)

Where, $n$ is the number of taps, $h_1(t-t_1)$ is the channel coefficient of the first tap, and $h_2(t-t_2)$ is the channel coefficient of the second tap and so on.
The real and imaginary part of each tap is an independent Gaussian random variable with mean 0 and variance 1/2. The term $\frac{1}{\sqrt{N}}$ is for normalizing the average channel power over multiple channel realizations to 1.

V. BER OF OFDM SCHEME

BPSK is the simplest form of PSK. It uses two phases which are separated by 180° and so can also be termed 2-PSK. The theoretical BER expressions for BPSK signaling in AWGN and Rayleigh channels are respectively given as [8].

$$p_b = \frac{1}{2} \text{erfc} \left( \frac{E_b}{N_0} \right)$$

$$p_b = \frac{1}{2} \left( 1 - \sqrt{\frac{E_b}{N_0}} \right)$$

Where $E_b/N_0$ is the energy per bit to noise power spectral density ratio.

VI. SIMULATION RESULTS

The performance analysis of OFDM has been carried out in term of BER as a function of (energy per bit to noise ratio). The BER performances of the proposed OFDM scheme are examined by using MATLAB simulation. The simulated system uses 52 subcarriers with 64-point FFT for 10000 transmitted OFDM symbols and 10 number of taps for multipath Rayleigh channel, since each OFDM symbol convolves with a 10-tap Rayleigh fading channel. In the given OFDM system, BPSK is the digital modulation technique and the channels are AWGN and Rayleigh fading. The different CP lengths in term of samples is applied in [3, 9]. These references used CP length (2, 4, 8, 16... etc.) samples, where the cyclic prefix consists of the last few samples of the OFDM symbol that are copied in front of the data block. Therefore the BER performance is presented with different CP length of samples (2, 4, 8 and 16) for both considered channels. The theoretical and simulated results are shown in Fig.6 and Fig.7. These figures are indicated the effect of varying CP is negligible in AWGN channel because there is no multipath signal and it is significantly varies in Rayleigh fading channel. Hence, the BER performance improves as much as CP length increases. In Fig. 7 at CP=16 samples, this value equal to a quarter of the length for the Fast Fourier Transform (N=64). The performances of the system for the Rayleigh fading and for the guard interval with a length equal to a quarter of the length for the Fast Fourier Transform are in accordance with the theoretical ones [10] for a maximum channel delay spread of delay intervals due to 10-taps. Therefore, the BER gives better performance than the other CP values and approaching the theoretical curve. The signal to noise ratio ($E_b/N_0$) difference between OFDM/CP AWGN system and OFDM/CP Rayleigh system shown in Fig. 8 is approximately 9.8 dB, for a BER=$10^{-2}$, and it increases for the lower values of BER. In this figure, the simulated result considered CP=16.
VII. CONCLUSIONS

This paper analyzed the effect of different cyclic prefix length on OFDM in terms of bit error rate probability for AWGN and fading channel. In case a communication channel is only affected by an AWGN the length of CP not influence the performances of the OFDM systems. Furthermore, the results of the simulations overlap with the theoretical results, also due to the fact that in an OFDM system which is affected only by AWGN there is no multipath propagation. Whereas, for high value of the CF, performances are better in Rayleigh fading channel as compared to AWGN channel. Therefore, once the prefix length decreases, the effect of the inter-symbol interferences over the BER is significant, leading to a degrading the system performance.

REFERENCES

Development of an IoT-based Noise Monitoring Network

Aram Mohammad Abdulqadir, Mohammed Hussein Shukur
Department of Computer Science
Cihan University - Erbil
Erbil – Iraq
E-mail: {aram.m@cihanuniversity.edu.iq, m.kurd@hotmail.com}
DOI: 10.24086/cocos17.13

Abstract—In this paper, we proposed an IoT-based sound pollution checking system. It is a method of an economical acoustic sensor developed on the Raspberry-Pi, for its use in the analysis of the noise level in the classroom. This prototype is connected to an online server to share results in the actual time. This experiment has shown the Raspberry-Pi as an impressive and low-cost computing core of an affordable device to evaluate the environmental sound pollution that affects student satisfaction and performance in higher education classrooms.

Keywords- Noise Monitoring; Smart Classroom; Noise Awareness; IoT; Raspberry Pi

I. INTRODUCTION

While at university students are exposed to various types of noise including external, environmental noise and noise generated within the classroom. Earlier researches have shown that sound-pollution has detrimental effects upon students’ performance at university, including reduced memory, motivation, and learning capability. The noise impact on student and their lecturers have been inspected by researchers in the past 40 years. It is generally accepted that noise has a detrimental effect upon the cognitive development of students.

Noise pollution is the inordinate noise measure or pesky sounds that unsettle students and distracting them in the lecture halls and workplaces. This kind of pollution has different effects on students’ health, physically and psychologically [1]. Main sources of noise pollution inside campus are high volumes of outside traffic and human-based sounds.

Recently, there has come into a new concept of computers. These new devices are also known as Single Board Computers (SBC) [2], being smaller than classic computers and with the differentiating feature of being more economical and affordable. This new kind of small computers has illustrated its computing power together with its scalability for real projects [3]. There are different SBCs in the market with different capabilities of connectivity, computing power, size or power efficiency. Raspberry-Pi, ASUS Tinker Board, Intel Edison, Arduino are widely used in this development area [4].

The role of acoustic researching in the smart classes has a series of applications and advantages such as having more control of noise levels by permanent and real-time control, detecting new noise sources or using these tools as a showcase to warn the lecturers and responsible people. From the viewpoint of classroom-administration, it helps lecturers to have plan to more control and try to get concentration of students’ within the lecture time. The investment and maintenance costs in this kind of devices are more economical than carrying out strategic noise maps repeatedly.

In classrooms, the noise levels are equal to residential environments and accepted are those which do not exceed 65 dBA during the day [5]. Accepted standards for recommended permissible exposure time for continuous time weighted average noise, stated that for every 3 dBA over 85 dBA, the permissible exposure time before possible damage can occur is cut in half, e.g., 85 dBA is linked with a permissible exposure time of 8 h; 88 dBA for 4 h, 91 dBA for 2 h [6]. The use of percentile levels in the acoustic analysis helps to have an understanding of the noise fluctuations over time. These are commonly used for environmental noise monitoring, such as road traffic or community noise assessments. With the use of long-term measurements, changes on the levels can be observed from the data, and more advanced studies can be performed in order to evaluate the noise volume.

Monitoring these sources of noise pollution is crucial for the comprehension of how these sounds evolve with time, in order to study it, control it and prevent it.

The work presented in this paper describes the creation of an advanced acoustical sensor connected to a Raspberry-Pi-3. It aims to fill the gap in the noise sensors research and developing field, with the analysis and monitoring of the noise signal in the audible bandwidth. It also calculates the environmental audio parameters done on-board instead of in a remote server. The device also shares the results in an Internet-of-Things (IoT) publishing online platform. The result of the research and development carried out in this paper is a reliable prototype, developed utilize low-cost components, of an advanced acoustic sensor for environmental noise analyzing.
II. MATERIALS AND METHODS

A. Design and Requirements

The design of the device had to perform few necessities for obtaining the final proposed aims. Some statements have to be achieved in until to follow the economic, but dependable, final device. The requirements for this prototype were:

- The device has to utilize cheap parts to develop and make low-cost sensor networks of several devices with a reasonable cost.
- The device has to have trustworthy for long-term measurements.
- The device should have capability to be connected to the cloud for remote updates of the software and for sharing results.
- The quality of the measurements has to be enough for advanced audio parameters’ calculation.
- The device has to have enough computing power to do on-board calculations.
- The device has to be able to connect to the peripherals needed for the purposes of the project (e.g., a microphone).
- The device has to be able to interpret Python programming language.
- The sound flow acquisition has to have the less noise inputs as possible, for avoiding extra filtering steps.
- The final device has to be protected against outdoor conditions using a protective housing.
- The device needs to have different connectivity options (i.e., Wi-Fi or Ethernet).
- The distance from the nodes to the Access Point (AP) should be a maximum of 200 m.

B. Selection of the Components

The main component of the device is the main-board processing unit, which is also used for the attainment of data and the connectivity. For reaching the requirements, the design of the noise checking and analyzing device was based in a Raspberry-Pi-3 Model B single board computer [7]. The Raspberry Pi platform offers a number of superiority as its good computing power, its high versatility and the existence of libraries of Python functions. The power efficiency and the cost give opportunity to create numerous devices based on this platform, resulting in economic and long-range nodes. Those capabilities made the Raspberry-Pi-3 the most suitable SBC for the development of a working prototype.

In this project, by the help of General-Purpose Input/Output (GPIO) which is a generic pin on the integrated circuit of the Raspberry-Pi-3, a microphone which integrates an audio capture card itself, was chosen and connected through the GPIO ports.

- The Raspberry Pi

The advantage of using the Raspberry-Pi-3 is the capability of working under a free OS. Here for this device, a Raspbian distribution [8], a GNU/Linux OS distribution for Raspberry-Pi-3, has been installed. The algorithms were developed in Python. The Internet connection of the device also provides the possibility of remote connection, with the help of SSH (Secure SHell) [9]. Through a terminal by typing a command it is possible to have access to the Raspberry-Pi-3 and modify the algorithms, software maintenance jobs or checking the system can be done from remote places. pyAudioAnalysis library [10] controls the audio configurations, managing the audio in an optimized way.

Based on the bandwidth requirements for continuous information transmission, the board allows different options. In the case of this device and its deployment, the option of the Wi-Fi (IEEE 802.11n) connection was chosen. The use of a Wi-Fi connection in the deployment instead of an Ethernet LAN seeks for two main objectives: first, while a wireless connection is subject to more freedom degree to than a wired connection regarding the location of installing device. And Ethernet cables may make untidy and cost more than Wi-Fi connection, so for proper communications and avoid these problems wireless connection is preferable.

In this way, a microphone with integrated board has wired to the Raspberry-Pi-3 board. A wireless Access Point (AP) is responsible for establishing the connection between the device and the Internet.

The Raspberry-Pi-3 board has powered by a 5 volt -2.5 amps power supply. And the whole microphone board getting the power from the Raspberry-Pi-3 board. The connection and arrangement in figure-1 has shown as follow.

![Figure 1. Operation scheme for RB-Pi-3, Sensor (Microphone) and connectivity via Internet.](image)

The code has developed in Python programming language. In Figure 2, a complete block diagram of the whole acoustic device is presented, where all the functioning blocks of the system are shown. One of the inputs of the system is the acquisition of the sound by the microphone sensing and capturing the environment sound and converting the analogue-sound-signal to a digital-signal with the sound card integrated in the microphone. Then it goes to the Raspberry-Pi-3 processing stage for the parameters extraction. Next, the data are formatted to send the parameters in real time to the server if...
noise level crosses the threshold. Then the lecturer gets awareness from the server.

The notification to the lecturer receives notification on his Computer or Mobile including status of his classroom and which parameters of his classroom have exceeded from the standard level.

Figure 2. Block diagram of the complete system. The inputs of the system are the sound acquisition that goes through the T-Bone GC100. Raspberry-Pi-3 Model B, is in charge to remove power line noises. Then it analyzes the signals and in case of abnormal situation it sends the status to the server.

III. ALGORITHMS IMPLEMENTATION

The Raspberry-Pi-3 Model B platform was chosen as the core of the device because it is multi-propose and has high versatility. Implementation is easy and the algorithms using a known and wide spread programming languages. Here Python language has used for this propose. The audio acquisition was made through pyAudioAnalysis which uses a portion from the Raspbian kernel meant to prepare and supply the system with audio functionalities, e.g., automatic configuration for sound-cards and the controlling of devices using one Linux system [10]. It is possible to configure features for the audio capturing like the rate of sampling and the size of the frame, which is the number of samples in each sliding window. Once the audio capturing is configured, analyzing the sound level starts in order to monitor the noise level of environment.

To calculate the audio level, the signal is acquired in a linear way, i.e., instant pressure values. So next step is conversion to a logarithmic scale. In order to summarize how sound is heard and measured.

Sound Pressure Level ($L_p$) - Sound is usually measured with microphones responding proportionally to the sound pressure. The power in a sound wave goes as the square of the pressure. (Similarly, electrical power goes as the square of the voltage.) The log of the square of $x$ is just $2 \log x$, so this introduces a factor of 2 when we convert to decibels for pressures. Sound Pressure Level can be expressed as: [11]

$$L_p = 10 \log (p^2 / p_{ref}^2)$$

Where

- $L_{eq} = \text{equivalent sound level (dB)}$
- $T = \text{time period (s)}$
- $p_A = \text{sound pressure (Pa, N/m}^2\text{)}$
- $p_{ref} = \text{reference sound pressure (2 \times 10^{-5} \text{ Pa, N/m}^2\text{)}$}

The maximum acceptable sound pressure level in classrooms which is acceptable is less than 30 dBA based on $L_p$ equation. [12]

For this first prototype, it has been equipped with Internet connectivity through an Ethernet connection and this capability has been exploited to store and show the results of the extracted acoustics parameters. This task has been carried out using an online platform called Cayenne. It is a free IoT application and Application Interface to store and retrieve data from the devices using the Hypertext Transfer Protocol and MQTT over the Internet [13]. Moreover, the platform enables the creation of sensor logging applications with status updates.

IV. RESULTS AND DISCUSSION

In this work, the design of an acoustic sensor designed which is low-cost but reliable. All of the components and its deployment in a pilot test have been presented.

At the first part, the design of sensor and its components has shown. The methodology to build the algorithm and the cloud connection in real time are explained.

The audio capturing in high resolution allows us to get more advanced results, like the psychoacoustic parameters as a future outcome. Also the power of the Raspberry-Pi-3 as the
core of the device gives the possibility of doing the calculations on-board, instead of sending the raw data to a sink node or a server for doing the calculations. So even in the case of network loss still the lecturer will be aware of high level of noise in the classroom.

In a second part of the paper, a pilot test where two devices were deployed was validated. In this deployment, the two devices were working and publishing the results in the real-time in an IoT publishing platform. The analysis of the sound field in long-term measurements inside the device with on-board calculations and the sending and publishing of the data obtained with ease and precision have been achieved. Like an innovative challenge, and through a research process, this sensor has been used for environmental acoustics parameters calculation and for being a platform where the inhabitants of the neighborhood could check the noise levels of their place. This makes the deployment as a tool for noise awareness, apart from simply a tool for gathering data with research purposes.

The platform and methods have chosen for the software development offers some advantages such as a great versatility, a low price for the components and a big simplicity for integrating the final device in classroom, being capable of turning into part of a sensor network as a node.

V. CONCLUSIONS

In other studies of the authors [4], low-cost platforms for ambient noise acquisition were proposed without on-board calculations without connectivity. In this work, a fully functional sensor with cloud connectivity has been proposed and tested. Extra features of on-board calculations, real-time data presentation and online access has included as well.

The Raspberry-Pi-3 has proved to be a powerful, versatile and economic computer that can be integrated in a sensor network scheme. Thanks to its connectivity options and the GPIO pins, a standalone computing device for premium sound acquisition and noise monitoring platform connected to the internet have been proved to be feasible. Based on the hardware and the software development for the algorithms and connectivity, it has been exhibited by creating a full functional which developed and tested and it is capable of creating a sensor network with Raspberry-Pi-3-based nodes and even more environmental sensors. We implemented a simple customized sensor node for achieving a high level of quality in teaching classrooms also these sensors can be used for detection of occurrence of emergency cases.

REFERENCES

Satellite Link Budget Calculator by Using Matlab/GUI

Adil Hussein M. Al-Dalowi
Communication and Computer Engineering Department
College of Engineering, Cihan University, Erbil
Adil.mohanned@cihanuniversity.edu.iq

Abdulqadir Ismail Khoshnaw
Communication and Computer Engineering Department
College of Engineering, Cihan University, Erbil
adrabdulqadir@cihanuniversity.edu.iq

Ghassan A. QasMarrogy
Communication and Computer Engineering Department
College of Engineering, Cihan University, Erbil
ghassan.qasmarrogy@cihanuniversity.edu.iq

DOI: 10.24086/cocos17.11

Abstract- In this paper, a satellite link budget calculator was done by using MATLAB – GUI program, the link budget is represented in one active screen, and it is designed to show the parameters that affects the RF signal when it is passing through the three main parts of the satellite communication system and regardless of the input signal power level. The results of the link budget program with the effects of changing the parameters will be shown inside the same active screen, which makes the users (students and trainers) analyze the reason that causes the weak signal when it reaches the satellite receiver.

Keywords: Satellite link budget, GUI, Simulation, gain margin, satellite link statues.

I. INTRODUCTION

Nowadays, satellite communication systems are evaluated and tested by using simulation programs which adds the environmental factors that affects the signals and observes the performance of the satellite link. A RF satellite link consists of an uplink (transmit earth station to satellite) and a downlink (satellite to the receiver earth station). The signal power and quality over the uplink depends on how strong the signal is when it leaves the source (earth station) and how the satellite receives it. While, on the downlink side, it depends on how strongly the satellite can retransmit the signal and how the ground station receives it. The signal from the source in the ground station will processes the signal to reach the satellite. The sending process contains modulation, frequency conversion and amplification, then it will transmit the signal to the satellite by a narrow beam antenna. Through the free space attenuation and massive loss appeared effect on the signal, so a weak signal will be received by the satellite. Signal amplification and some processing is needed to convert the signal from uplink frequency to down link frequency. Many studies were done with different methods such as RF link budget - Simulink -MATLAB, which shows the effects of the power level, antenna gain and S/N ratio only [1]. RF- café offers a program named RF calculator workbook by excel, and it deals with main factors of the link budget and calculates the power received [2].

In this paper, the net power transmit from the earth station will be calculated in consideration with the main factors which makes the loss and attenuation in the path for the signal before transmitting on the free space channel. This paper shows all the factors affecting the signal on the receiver side, and the factors that gives the again and loss on the signal. Finally the results will show the effects of all factors and calculates the status of the satellite link.

The rest of the paper is organized as follows, section 2 explains the RF satellite link budget program, section 3 demonstrates the sending signal and what follows, section 4 shows the analysis and the result of the program, and finally section 5 concludes the paper.

II. RF SATELLITE LINK BUDGET.

The purpose of a satellite system is to provide reliable transmission with a specified quality of the received signal. The transmitted information has to be modulated on an RF carrier. In analog systems, the frequency modulation (FM) is the dominating modulation method, the signal-to-noise ratio (S/N) after the demodulator is the measure of signal quality. In digital satellite links, the measure of quality is the bit error rate (BER). The modulation method mostly often used in digital system is phase shift keying (PSK). In both analog and digital systems, there is a unique relationship between the carrier-to- noise ratio (C/N) and the signal-to-noise (S/N) ratio or the bit error rate (BER). Given the modulation method, the
The performance of the total link is generally specified in terms of a minimum C/N in a certain percentage of time. In order to establish the link quality, we need to calculate the carrier power (C) and the noise power (N) at the receiving station. [3].

Figure (1) shows the main parts of a satellite communication system (uplink), where each part contains a block can be represented as mathematical model by simplifying their function or the process needed on the transmitted signal.

Figure (1): Main Block Diagram of Satellite Communication System

The link budget calculation are usually made using decibel (dB and dBm), the transceiver designer’s objective is to close the link for the specified distance and required availability as efficiently as possible, whereas the link designer’s task is to use an existing transceiver to satisfy a specific communication requirement. The link designer may then trade off availability for link distance.

### III. TRANSMITTER STATION

The discussion in this section is about the ground station, the main process on the signal will be to modulate the signal or change the form of the signal then it is to convert the band of the signal from intermediate frequency band L- band to C, X or Ku band, then amplifying the signal by power amplifier to increase its amplitude and its power. After that the signal is directed to the satellite by a reflector antenna, which gives the signal extra gain with respect to isotropic radiation, that signal called (power flux density), which radiates in a given direction by any antenna that have gain GT, the equivalent isotropic radiated power (EIRP) is:

$$EIRP = PT \cdot GT \text{ (in watt)}$$

or

$$EIRP = PT \text{ (dB)} + GT \text{ (dB)} \text{ (in dB)}$$

GT can be calculated in the following equation

$$GT = \eta \cdot (10472 \cdot D \cdot F)^{\frac{1}{2}}$$

Where $\eta$ is the aperture efficiency which has a value (0.5 to 0.65), $F$ is the carrier frequency in (GHz), and $D$ is the reflected antenna diameter in (m), or by using the equation (4) to calculate GT or GR, along with the carrier frequency in (MHz).

$$GT \text{ dB} = -42.2 + 20 \log F \text{(MHz)} + 20 \log D \text{ (m)}$$

with typical value for aperture efficiency is (0.55) [4].

Adding to that, some kind of loss must be consecrate in this stage like modulation process loss, connection and cable loss,

$$EIRP = PT \cdot GT - Lt \text{ in (dB)}$$

Where Lt is total of transmission loss in dB.

### IV. SPACE CHANNEL PART

The biggest attenuation on the signal happens in this section. Where the constitute path losses in the link equations. These losses include system loss (due to thermal noise), transmission loss due to ionosphere (cloud, rain, fog and gazes), and directional (pointing) loss.

Free space loss (FSL) have two important factors which are frequency $F$ and the range $R$ or distance between earth station and the satellite, so that, it can be calculated by the following equation:

$$FSL \text{(dB)} = 32.4 + 20 \log R + 20 \log F$$

Where $R$ in Km and $F$ in MHz [5]

The other losses also must be considered for final calculation, and these are simply added to FSL. The losses for clear –sky condition is

$$\text{Total losses dB} = \text{FSL+AML+AA+ PL}$$

where AML is antenna misalignment loss in (dB), Anais atmospheric absorption loss in (dB), PL is polarization mismatch loss in (dB), and some other loss such as cables and connectors loss in the transmitter and the receiver, that will call as (Rx) in (dB).

### V. NOISE AND NOISE FIGURE

Receiver noise includes contributions from thermal noise, short noise and possibly flicker noise. These may arise in the input RF section of the receiver. The total receiver noise $Tso$ can be calculated from the following equation.

$$TS = TRF + Tin + Tm/Gr \text{ in (K)}$$

Where TRF is the temperature on the front end of RF part in the receiver, Tin is the input temperature to the receiver, Tm is the frequency convertor unit or the mixer temperature, all in Kelvin (K), and Gr antenna gain. An alternative way of representing amplifier
noisy is by means of its noise factor, F. In defining the noise factor of an amplifier, the source is taken to be at room temperature, denoted by $T_0$, usually taken as 290 K. The noise figure can be calculated by this equation

$$F = \frac{T_S}{T_0} + 1$$

Or

$$F(\text{dB}) = 10 \log F$$

Noise power depend on the bandwidth of the receiver ($B$) and noise figure ($F$) so the noise power is given by

$$N = k T_0 B F \text{ in(watt).}$$

$$N(\text{dB}) = -174. \text{ dB/Hz} + 10 \log (B) \text{Hz} + F \text{ dB}$$

Or

$$N(\text{dBm}) = -114. \text{ dB/MHz} + 10 \log (B) \text{MHz} + F \text{ dB}$$

**V.1. FIGURE OF MERIT G/T**

The $G/T$ ratio is a key parameter in specifying the receiving system performance. The antenna gain $G_r$ and the system noise temperature $T_s$ can be combined in the following equation

$$G_r \text{ dBi} = -42.2 + 20 \log F \text{MHz} + 20 \log D_m$$

$$G/T \text{ dBi} = G_r - 10 \log T_s$$

by adding antenna receiver Rx loss in (dB) to $G/T$, then

$$G/T \text{ dBi} = G_r - 10 \log T_s - \text{Rx loss}$$

Signal power received (PR) can be calculated by the following equation

$$PR = \text{ERIP} - \text{total losses} + G/T$$

That power must be greater than minimum signal power requires (C min) to the receiver.

**V.2. LINK BUDGET ANALYSIS**

A measure of the performance of a satellite link is the ratio of carrier power to noise power at the receiver input, and link-budget calculations are often concerned with determining this ratio. Conventionally, the ratio is denoted by $C/N$ (or $\text{CNR}$), which is equivalent to $\text{PR}/N$. In terms of decibels,

$$C/N \text{ dB} = \text{PR} - N$$

The Link Margin obtain which tells how tight we are in closing the link:

$$\text{Margin dB} = \text{PR} - \text{C min}$$

The allowed margin depends on the required reliability (eg. link maintained for $(99.99\%)$ of time, averaged over one year) and the range of climatic conditions which are predicted along the link. Typical margin values are $2\text{dB}$ (C band) and $8\text{dB}$ (Ku band) [6]. The link status depends on the value of link margin, which will be close for positive value, that means the system is working well, and if the negative value for the margin is open, it is means that the system is not working.

**VI. SIMULATION OF THE RF LINK BUDGET**

This program is designed to show all the input and output parameters together on an active screen in order to study the effects on the output results when one or more parameter is changed. The program has many variables that must be given to that program, such as the following parameters which are shown in table (1).

<table>
<thead>
<tr>
<th>Table (1) input measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input parameters</strong></td>
</tr>
<tr>
<td>Operating frequency $F$</td>
</tr>
<tr>
<td>Output power $P$</td>
</tr>
<tr>
<td>Transmitter Antenna Diameter $D$</td>
</tr>
<tr>
<td>Loss in antenna complex $TX$ Loss</td>
</tr>
<tr>
<td>Operation bandwidth $BW$</td>
</tr>
<tr>
<td>Modulation loss $Mod Loss$</td>
</tr>
<tr>
<td>Slant range $R$</td>
</tr>
<tr>
<td>Atmosphere loss $AA$</td>
</tr>
<tr>
<td>Polarization loss $PL$</td>
</tr>
<tr>
<td>Antenna misalignment loss $AML$</td>
</tr>
<tr>
<td>Threshold level $dBm$</td>
</tr>
<tr>
<td>Satellite antenna diameter $D$</td>
</tr>
<tr>
<td>Receiver loss $RX Loss$</td>
</tr>
<tr>
<td>Equivalent temperature $Te$</td>
</tr>
<tr>
<td>Reference temperature $TO$</td>
</tr>
</tbody>
</table>

Then the program is going to calculate the require parameters which are shown in the table (2).
Table (2) output measurements

<table>
<thead>
<tr>
<th>No</th>
<th>Output measurements</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wave length</td>
<td>Cm</td>
</tr>
<tr>
<td>2</td>
<td>Antenna transmitter gain Gt</td>
<td>dBi</td>
</tr>
<tr>
<td>3</td>
<td>ERIP</td>
<td>dB/m</td>
</tr>
<tr>
<td>4</td>
<td>Free space loss FSL  loss</td>
<td>dB</td>
</tr>
<tr>
<td>5</td>
<td>Total space loss</td>
<td>dB</td>
</tr>
<tr>
<td>6</td>
<td>Antenna receiver Gr</td>
<td>dBi</td>
</tr>
<tr>
<td>7</td>
<td>Figure of merit G/T</td>
<td>dB/K</td>
</tr>
<tr>
<td>8</td>
<td>Received power Pr</td>
<td>dB/m</td>
</tr>
<tr>
<td>9</td>
<td>Noise figure</td>
<td>dB</td>
</tr>
<tr>
<td>1</td>
<td>C/N</td>
<td>dB</td>
</tr>
<tr>
<td>1</td>
<td>Gain margin</td>
<td>dB</td>
</tr>
<tr>
<td>1</td>
<td>Link status</td>
<td></td>
</tr>
</tbody>
</table>

After entering the parameters, the program decides if the link is closed or not. Depending on the condition that if PR is greater than the threshold level the link is closed, and if PR is less than threshold level the link is open. [7] . The link status depends on the value of link margin, it will be closed for positive value, that means the system is working well, and negative value for the margin is open and it is means the system is not working. By using GUI/ MATLAB program to design the simulation, the graphical user interface (GUI) is a graphical display in one or more windows containing controls, called components that enables the user to perform interactive tasks. The user of the GUI does not have to create a script or type commands at the command line to accomplish the tasks. Unlike coding programs to accomplish tasks, the user of a GUI needs not to understand the details of how the tasks are performed.

The figure (2) shows the final active screen of satellite link budget simulation, the white color fields for the input parameters and blue sky color for useful output parameters which are using in link budget equations.

**VI.1. RESEARCH METHODOLOGY**

The following steps shows the procedure for the analysis of a satellite link:

1. Run the MATLAB program.
2. Call GUI file then open it (our simulation file).
3. Write the value of the uplink carrier frequency.
4. Select the transmission powers.
5. Choose any value for antenna diameter.
6. Estimate the loss in transmitter such as cable loss and connectors.
7. Estimate the loss for modulation. Write the range of the satellite.
8. Give a value for antenna misalignment loss.
9. Give a value for polarization loss.
10. Estimate the loss in free space or atmosphere loss such as (rain, gas and foggy).
11. Give a value for minimum signal required to the receiver.
12. Chose the diameters for the satellite antenna.
13. Give a value for receiver loss.
14. Write the reference temperature.
15. Write a value system temperature (of the noise temperature) then Click on calculate key. The figure (3) has shown the active screen after feed all input parameters.

**VI.2. THE RESULTS**

The results shown in the figure (3) shows how the program calculates the parameters which are shown in the table (2), the results with all input parameters will show in the active screen. As shown in figure (4). On the same screen. The value of any parameters can be changed then click on (calculate key), the results will change according to the new value, for example, the
AML Loss is changed from 1 to 2 the result also change as shown in figure (5), same thing if AA change from 0.5 to 4 such as a heavy rain, the figure (6) shown the results ware change. And so on.

The simulation of the satellite communication and their parameters. The dynamic of parameters of the system and see the effects at the users to examine the effects of all the parameters on the result shown changes on the outputs.

AML Loss is changed from 1 to 2 the result also change as shown in figure (5), same thing if AA change from 0.5 to 4 such as a heavy rain, the figure (6) shown the results ware change. And so on.

The simulation of the satellite communication and their parameters. The dynamic of parameters of the system and see the effects at the users to examine the effects of all the parameters on the result shown changes on the outputs.

The simulation of the satellite communication and their parameters. The dynamic of parameters of the system and see the effects at the users to examine the effects of all the parameters on the result shown changes on the outputs.

The program covers the requirements of the satellite laboratory for experiments of the design and analysis of the RF link budget for overall system which it can show the effects of all input parameters on the output results. The simulation of the satellite link budget by using MATLAB/GUI, gives us some extra flexibility to prove and sense the relationship between some parameters in the link budget calculation. Unlike the RF Satellite Link example in MATLAB that have two variables SNR and Adaptive Noise, our program have thirteen variables and it will show the changes in all the important parameter when changing any variables. The simulation is open source available for other users to add or modify the system for any development in the future.

The final results were evaluated with a referenced with results from an international company web site which is used to examine their product in the same field [8].

REFERENCE

Enhanced Situational Awareness and Security Assessment in Surveillance Systems Using Cloud Model Theory

Abdulqadir Ismail Khoshnaw, Ph.D
CIHAN University - Erbil
Department of Communication and Computer Engineering
drabdulqadir@cihanuniversity.edu.iq

Adil Hussain Mohammed Al-Dalowi, MSc
CIHAN University - Erbil
Department of Communication and Computer Engineering
Adil.mohanned@cihanuniversity.edu.iq

Ghassan A. QasMarrogy, MSc
CIHAN University - Erbil
Department of Communication and Computer Engineering
Ghassan.qasmarrogy@cihanuniversity.edu.iq
DOI: 10.24086/cocos17.14

Abstract—Cloud Model Theory is a mathematical method to model the two components of uncertainty, Randomness and Fuzziness in linguistic concepts. This paper introduces a method to assess information, make and fuse decisions in multi-layered sensing systems using the cloud model to process uncertainty. In this research, Cloud model theory is used to model information extracted from digital images taken for the purpose of monitoring and surveillance in multi-layered sensing systems. The extracted information is assessed using the cloud models to make decisions about the level of security situations in the area under surveillance. The threat level of any security situation can be considered as concepts and can be modeled using cloud models to produce assessments; these assessments are then fused to make a decision about the level of the security threat. Cloud models provided a robust methodology to make decisions and evaluate security situations which led to enhanced situation awareness. Test results showed that cloud models performed much better in comparison with just using standard fuzzy logic models.

Keywords-Cloud Model Theory; Situation Awareness; Layered Sensing Systems; Information Assessment; Decision Making.

I. INTRODUCTION

The use of wireless sensor networks has expanded to many engineering application areas such as military applications, indoor and outdoor environmental monitoring, support for logistics, robotics, health systems, etc. [1, 2]. Military or civilian surveillance systems are designed to provide better situational awareness to the operators and decision makers. This task faces many challenges in terms of sensor technology, computation, communication, and human operators. The challenge of human operators is a serious limitation on using surveillance system efficiently because of tiredness, fatigue, lack of attention, etc. [3]. To solve this problem, attempts were made to introduce intelligence to surveillance systems in order to automate data fusion and information assessment especially in multi layered sensing systems [4].

Besides using probability theory to deal with uncertainty in information, new concepts were introduced to treat fuzziness and randomness in information. The efforts of Lotfi Zadeh has produced new concepts and a new way of thinking in human capability to do calculations using linguistic concepts without numbers. Humans don’t have precise measurements when making a decision in a situation that requires
assessment. These new concept lead to new methodologies for information assessment such as computing with words and cloud computing. [5, 6].

The research described in this paper introduces one such attempt to assess information in a multi-layer surveillance system using cloud model theory to deal with the uncertainty in the information in order to make decisions about threat situations in an area under surveillance.

This paper is organized as follows; Section I will is an introduction to the subject, Section II will explain the cloud model theory, Section III will explain the methodology of extracting information from images and how to model it using cloud models, Sections IV discusses the results and the analysis of the results, Section V presents the conclusion of the research efforts, and finally future direction of the research area is presented in Section VI.

II. Theory of Cloud Modeling
Professor Deyi Li described a new method called cloud model theory to deal with randomness and fuzziness in a linguistic concept by creating a relationship between qualitative concepts and quantitative values. This model introduces a method to transform qualitative concepts to quantitative values [6]. The idea behind a cloud model states that any linguistic concept can be represented by a cloud graph and this graph can be utilized to get assessments about any data point of the information. The linguistic concept is defined as a cloud and any data point is defined as a cloud drop [6]. The summary of the cloud model theory states that if (C) is a quantitative concept that is represented by the set of numbers (U), if we take a number (x) which is a member in (U) and realizes the concept (C) then the confidence degree of (x) for (C) is defined by a random value \( \mu(x) \) which is between 0 and 1. This random value has a stabilization tendency shown in equation 1.

\[
\mu: U \rightarrow [0,1] \quad \forall x \in U \quad x \rightarrow \mu(x) \quad (1)
\]

The distribution of x is represented by a cloud, and every x represents a cloud drop [6].

In a cloud model, the properties of any concept can be represented by the numerical characters which are the overall quantitative property of the qualitative concept. In every cloud model three numerical characters can be employed: Expected value \( E_\mu \) which is the mathematical expectation of the cloud drop distribution, Entropy \( H_\mu \) which is the uncertainty in the concept, and Hyper Entropy \( H_\mu \) which is the second order entropy of the entropy [6]. Cloud models can be represented by Cloud graphs such as in Figure 1.

![Cloud Models Graphs](image)

(a) Half Cloud Model.
(b) Symmetrical Cloud Model.

**How to create a Cloud Model:** Cloud models can be created by using a forward and backward cloud mapping. A Forward cloud creation is the transition from quality (concepts) to quantity (values). This is done by representing the numerical characteristics of a concept \( (E_\mu, H_\mu, H_\mu) \) in a cloud graph. The cloud graph can contain a number of cloud drops \( x \) with known confidence degrees \( \mu(x) \). Backward cloud creation is the transformation from a quantitative value to a qualitative concept. In this cloud creation a number of \( x \) is selected and its confidence degree \( \mu(x) \) is extracted. The confidence degree \( \mu(x) \) is calculated by using equation (2) [6].
\[ \mu_i = e^{-\frac{(X_i + Ex)^2}{2(\sigma_i)^2}} \]  

(2)

\((Rn)\) is a random number generated from a normal distribution function.

III. SITUATION AWARENESS IN SURVEILLANCE SYSTEMS

Surveillance systems have advanced from monitoring camera systems using human observers to smart surveillance systems where advanced techniques and algorithms are used to help the human observer determine the threat level of any situation under surveillance. These systems still lack some decision making capability that can substitute the absence of human observer. The main objective of these surveillance systems is to provide complete situation awareness about any security threat that faces any facility under surveillance.

The research presented in this paper presents a new methodology to assess any situation under surveillance in terms of threat level. In this method a mathematical model is built based on the cloud model theory and is used to assess the threat level of any situation. This is done automatically and this way a new level of intelligence is added to the surveillance system. This provides a decision making capability that can be used to increase situation awareness for the system.

In this research cloud models were developed to assess the threat level. The assessment started with identifying security concerns as linguistic concepts for the areas under surveillance. The security concerns which were selected for experiments were geographical areas under surveillance and the objects in these areas. To create a cloud model for areas of interest, parts of the area were selected based on borders on the ground and these borders were modeled into a cloud model from an initial setting or an image. Objects in these areas were modeled into cloud models based on their identified features.

To create the cloud models, initial pictures were studied of the areas of interest and security concerns were identified and the mathematical characteristics \((E_x, E_y, H_x)\) were determined. A cloud graph was developed for each security concept and object of interest. An example of such process is shown in Figure 2.

![Fig. 2 developing cloud models for security concerned areas.](image)

(a) Initial picture of an area under surveillance.  
(b) Cloud model developed for area.

Information Assessment from security areas: The methodology for assessing threat level information from the security areas involved taking images from the area under surveillance and provide information extracted from the images to the cloud models designed for the area to assess security concerns or objects features. The assessment involved determining confidence degree \(\mu(x)\) for each threat level. Based on these assessments, a decision was made about threat levels for any event that happens in the area under surveillance.

In multi-layer surveillance systems, information assessments from different layers were fused for the same event to enhance the decision making process about threat level of an event.

Assessments from different layers can be combined using a two dimensional cloud model. The two dimensional cloud combines two confidence degrees using a soft- and logic instead of Boolean Logic.

IV. RESULTS AND ANALYSIS

The methodology of using cloud models for information assessment was implemented in a three layer surveillance system. Areas under surveillance were monitored from three layer camera system where images were taken of the area and analyzed for information that was used in the cloud models for assessment. Areas under
surveillance were classified into security zones and object features in these areas were identified and used to extract information from the images taken in these areas. Threat level assessment was classified into categories of threats ranging from low threat to high threat and each was assigned a range of confidence degree associated with uncertainty level.

To compare and analyse the cloud model theory based information assessment system, a parallel information assessment system was developed using standard fuzzy logic. The same information extracted from the images were assessed using both systems. From the analysis of the results of the tests scenarios carried out in both systems, the result showed that the cloud model based system performed much better than the traditional systems that are based on only fuzzy logic. The results were assessed from the human point of view about the decision made by the systems in terms of security situations the results showed that the cloud mode system missed the right assessment in 18% of the test scenarios only which shows that cloud model based system can obtain better results because of dealing with the information uncertainty with both elements of randomness and fuzziness present in the analysis. Results of the test scenarios are shown in Figure 3.

V. CONCLUSION

The objective of this research was to introduce a new methodology to autonomously assess information with uncertainty in multi-layer surveillance systems. The purpose of the information assessment was to help human operators and decision makers to detect threat levels more accurately.

Information assessment and decision making capabilities provided by the cloud model theory system produced accurate and acceptable results. Cloud models deployed in the system provided a way to treat the uncertainty in the information that every decision making system faces. The cloud model theory has an advantage because it can map quantitative concepts to qualitative mathematical models by combining information fuzziness and randomness in the same model.

The proposed system performed better in experiments compared to a similar system using only fuzzy logic to assess the information. This methodology of using cloud models for assessing information could be expanded to be used in many other areas when uncertainty is part of the information. One such area for using the cloud models is to develop a control mechanism for data quality control for heterogeneous sensor networks.

VI. FUTURE WORK

Adding a higher level of intelligence to systems has a great potential and is the a wide area of research in the field of intelligent control systems such as surveillance systems, manufacturing systems, automation systems, robotic systems, embedded systems, etc. It is the intention of the researchers here to continue the work in this area to develop a robust algorithm and methodology to introduce intelligent control systems for many applications such as irrigation systems, traffic control systems, home security, commercial surveillance systems, etc.
REFERENCES


Database Protection System Depend on Modified Hash Function

Alaa K. Farhan  
Computer Science Department  
University of technology, Baghdad- Iraq  
dralaa_cs@yahoo.com

Mohammed Abed Al-jabber Ali  
Computer Science Department  
University of technology, Baghdad- Iraq  
mo_force@yahoo.com

DOI: 10.24086/cocos17.15

Abstract— The aim of this research is to protect data using enhanced MD5 with 1024 bits length of input block message and output with 160 bits, by using multi techniques. Database is protected using two techniques; first, maintains the integrity of the data by relying on hash technique, as well as enhanced MD5 which is used to generate the password for users with a length of 160 bits; second technique is used to maintain the confidentiality of the data using AES algorithm to encrypt sensitive data.

Keyword: DATABASE, ENHANCED MD5, AES.

1. INTRODUCTION

There is a set of security demands for a data-base such as physical, logical, and element integrity in addition to auditability, access-control, user-verification, and data-availability. The safety of the actual database is concerned with physical issues connected to data such as power-outages base. Therefore, a data-base must undergo recovery from this type of problems. The integrity of the logical data-base is concerned with the management and preservation of the structures and relations in that data-base [1].

Cryptography is the technique of making the plaintext understandable by the unauthorized parity in which cryptology is made up of, while crypto-analysis (cryptanalysis) try undoing what cryptography attempts to do. [2]

Encryption is the procedure that modifies the message (or is other words the plain-text) for the sake of rendering it insignificant to everybody except the ones that are in possession of the decryption-key. The insignificant message (encrypted message) is typically known as the cipher text. Decryption is the opposite procedure that works on recovering the plain-text from the cipher text [3].

A hash function is a term implemented in the field of the computer sciences a long time ago and it means a function which performs a compression on a string of some input to a fixed-length string. On the other hand in the case where it meets a set of extra requirements, it can be utilized in cryptography applications and therefore called as hash-functions which are of the most vital tools of the cryptographic area and are utilized for achieving a set of security criteria such as authenticity, digital-signatures, pseudo-random number generation, digital steganography, digital time stamping and so on. [4, 5].

The rest of this paper is organized as follows: section 2 provides an overview of the related works, the proposed system details and implantation are presented in section 3, and section 4 presents the conclusions.

2. RELATED WORKS

The objective of this study is combining some function for the sake of reinforcing them and to increase the hash-code’s length up to 512 as well, which generates stronger algorithm to face the collision attacks. [6]

The protection and confidentiality of sensitive information in outsourced multi-relational databases is by improving an existing approach based on a combination of fragmentation and encryption. Then a secure and effective technique is defined for querying data hosted on several service providers. Finally, improve the security of the querying technique in order to protect data confidentiality under a collaborative Cloud storage service provider’s model [7].
Data security is an emerging concern proved by an increase in the number of reported cases of loss of or exposure to sensitive data by some unauthorized sources. Security is a composed part in which it protects and secures the sensitive data or database management software from some unauthorized user or from malicious attacks. In this paper we will be presenting some of the common security techniques for the data that can be implemented in fortifying and strengthening the databases [8].

3. PROPOSED SYSTEM FOR PROTECTING DB

The following subsections are discussing the implementation details of the proposed system.

3.1 SYSTEM ARCHITECTURE

In this proposed system, the database is protected using two levels. The first one, which is the responsibility of the system, which is relies on enhanced MD5 at the database to protect it against intrusion of the authorize parity, the second protection level is the encryption of sensitive data by the system administrator which is determined in advance based on the stored information about the official of encrypting a column based on AES block Cipher (Advanced Encryption Standard), the design of this system is based on the strength points of every key length of the this method (i.e. 128, 192 and 256 key length) which are efficient for protecting secret information.

3.1.1 Enhanced MD5

The enhanced method depends on multi techniques such as DNA coding, non-Linear Feedback Shift Register (NLFSR), and Logistic function of Chaos theory. Enhanced MD5 will expand the input of the algorithm to 1024 bits instead of 512 bits, and the output to 160 bits instead of 128 bit.

The complexity try’s to increase the data inputs by preprocessing before entrance MD5 operation, where, will use NLFSR and DNA coding in addition the use Logistic function of Chaos theory with each rounds of MD5. In the following steps, the proposed system based on enhanced MD5 will be explained. The Development which based on the MD5 includes amplified complexity against brute force attacks and increase the percentage of probability to know the explicit provision of attackers on the previous algorithm, figure (1) shows one block algorithm of the proposed algorithm.

3.1.2 Enhanced MD5 via classic MD5 for hash value

The enhanced MD5 algorithm applies to messages that have different size as (64byte, 128byte, 512byte, 1KB, 5KB, 10KB, 1M, 5M, and 10M) that encodes process of Milliseconds and the test message in five times for the sake of ensuring that results are clear due to the fact that the CPU can be involved in some other procedure. Table (1) explains the processing-time measured by the Milliseconds that was computed by subtraction from the time of starting the operation and the time of its ending.

Table (1): Time in Milliseconds

<table>
<thead>
<tr>
<th>File size</th>
<th>Classical MD5</th>
<th>Enhanced MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 byte</td>
<td>00:00:00.0002232</td>
<td>00:00:00.0002297</td>
</tr>
<tr>
<td>128 byte</td>
<td>00:00:00.0003828</td>
<td>00:00:00.0004023</td>
</tr>
<tr>
<td>512 byte</td>
<td>00:00:00.0005683</td>
<td>00:00:00.0005923</td>
</tr>
<tr>
<td>1KB</td>
<td>00:00:00.0006722</td>
<td>00:00:00.0006803</td>
</tr>
<tr>
<td>5KB</td>
<td>00:00:00.0007175</td>
<td>00:00:00.0008125</td>
</tr>
<tr>
<td>10KB</td>
<td>00:00:00.0007706</td>
<td>00:00:00.0007966</td>
</tr>
<tr>
<td>1M</td>
<td>00:00:00.0026558</td>
<td>00:00:00.0027326</td>
</tr>
<tr>
<td>5M</td>
<td>00:00:00.0033024</td>
<td>00:00:00.0034589</td>
</tr>
<tr>
<td>10M</td>
<td>00:00:00.0043451</td>
<td>00:00:00.0044295</td>
</tr>
</tbody>
</table>

Curves are used to explain the differences in time which have been illustrated in figure (2) below:
3.1.3 Complexity Enhanced MD5 via classic MD5

- The MD5 algorithm uses four round each one has sixteen steps, in enhancement add complexity to the round by using DNA coding, logistic function and NLFSR.
- Expand the size of the block message from 512 bits to 1024 bits in the enhancement of MD5 algorithm which led to maintain its speed.
- Generation key form polynomial primitive by using function having GF (2^32) this is generates max period number (2^32 − 1) binary key, that key is used for preprocessing message, in MD5 original doesn’t have key. Enhancement of MD5 puts DNA coding work to convert binary message with key that results from NLFSR in final output new message before entering round. That step is preprocessing message, in MD5 original not preprocessing found is just transposition inside round.
- The MD5 algorithm outputs 128 bits, enhancement algorithm outputs 160. No. Of attacks needed to find original message is 2^{128} bits operations required in MD5 original and needs 2^{160} bits operations.

3.1.3 First phase of Protection DB

The first phase of DB protection would be the responsibility of the system administrator to protect the database. In the first step, proposed system reads first record of table in database and performs the hash function by using the proposed MD5, then, this value is placed in a separate table on the main table for the database. The link between the hash value and the record is the value of prime key. After this step, the proposed system reads value of columns that will be encrypted by AES algorithm which selects data from the encrypted record and then is stored in the new database. Figure (3) illustrates the creation of hash table and the table of encrypted sensitive data. This process is done for all fields in the table, the system takes a period of time to create database protection file for the server and shared by users through such measuring as the base size and the number of records that the encryption key of AES generated which is based on the number of columns. For example, if the database contains ten columns, the system will generate ten keys; each key is different from the other. This step is exclusively the responsibility of the system administrator and not anyone else who had the authority to generate keys for encryption or log encryption.

Figure (2): Time of Hashing process.

Figure (3): Create hash table to protect database

To create an encrypted table for sensitive data in addition to creating a hash table from the original table, this will be lifted on the server. The following steps explain the steps of encrypted the DB tables:
1. Read table from database.
2. Read record of table.
3. Apply hash function of data onto the record by using enhanced MD5.
4. Encrypt sensitive data onto the columns by using AES algorithm.
5. Insert hash value in new table.
6. Save table after encrypting data onto new table.
7. Purpish database on server.

After creating a hash table and encrypt sensitive data by the system administrator, columns are encrypted depending on the data that can be filed for the type of server and shared with many users to take advantage of the data according to the nature of the query. Sensitive data encryption process maintains the confidentiality of data and encryption of table maintains the integrity of the data, figure (4) shows the flowchart of restructuring and creating a table of hash and encryption of sensitive.
3.1.4 Second phase of DB protection

After put the encrypted database with hash table on the server and work with the participation of everyone, this phase is applied. Here begins the role of the system to be protected, in this section the detailed steps to protect the database is explained also measures to ensure data integrity to deliver it to user with truth.

The common protections for the processes of protecting the database from unauthorized access to the system in all data systems are using user name and password.

The process of accessing the protected data base is through the introduction to user name and password. The password of hash function is processed by enhanced MD5 with size of 160 bites and matches them with passwords stored in the database and when matching the system allows access to the database to be able queries the data.

The operations conducted by users on the database vary according to their powers. This feature is not making all users have the same possibilities in the query and insertions and deletions and update the database.

In the event of the completion of registration of the system, the user can query within the database. The system administrator grants some users free access and limited to be held on the database. When the user name and password entered to the system, a matching process is taking place on the field of accesses to the user to not allowing him/her to hold operations on the system.

3.1.5 System Scenario

In figure (5), system works fully to illustrate the beginning of user login and conduct operations on the database until they return the result to ensure the protection for information.

The following steps describe the scenario of the proposed system:

1. Sends a query to the system.
2. The system receives query from the user if the search for specific data to be matched with the data onto the database.
3. Using SQL language to Search as “select * from * where?”, and return the result.
4. Connect the database with the system.
5. After obtaining the result from step (3), fetch all data of record.
6. Decrypt sensitive data and encoding the record by MD5 enhancement.
7. Connect with hash table and compare results from step (6) with hash store in the table to same record by id number.
8. Return results to compare process from hash table.
9. Return results to application.
10. If correct data with no any manipulation return results to user.

In Figure (6) illustrates the query structural data onto the database, when searching for data encrypted within the database system confirmed the query therefore if encrypted information encrypts the query and research and match. In this section the process of ensuring and match data onto the agenda for her not to make sure that the manipulation and, consequently, if the information was held by any slight change started examining the notice to the director of the system directly.
4. CONCLUSIONS

Oversized database is difficult to identify data that was manipulated by the attacker and determine the constraint that contains those statements, in the proposed system have the potential to determine constraint depending on the configured hash value (MD5 enhancement) for each constraint and matched with the original version. use MD5 enhancement increased to protect DB to access control, where encoding password has user by it and don’t need to add salt to original algorithm when encoding password user in system traditional. Also grants the administrator the flexibility to encrypt sensitive data which reduces the time spent in answering in the program spend in search and decrypt database, the system is a security system help to administrator determine the powers and responsibilities of users to ensure that no tampering by spirited.

Disadvantage of proposed system is the size increment of database by adding tables contain the hash value for each entry and attached file size in algorithm which contains the keys to the size $2^32$, through step enhanced MD5 faced slaw of speed the process after adding complexity to it and process by expend block input to 1024 instead 512 to keep of speed the algorithm.

REFERENCES


The Impact of Information Security International Standards
Enhancing the Efficiency of E-Publishing over Cloud Computing

Thabit H. Thabit
Dept. of Control and Internal Audit
Ninevah University
Mosul, Iraq
thabit.acc@gmail.com

Yaser A. Jasim
Dept. of Accounting
Cihan University
Erbil, Iraq
yaser.a.jasim@gmail.com

DOI: 10.24086/cocos17.16

Abstract— This paper aims to determine the role of international standards for data security to increase the efficiency of E-Publishing over cloud computing by a case study to a sample of academics and researchers, and to achieve the objectives of this paper a questionnaire was developed to gather data from samples and analyze these data by using fuzzy logic tools, it also pursuits to add knowledge to E-Publishing, its concepts and the role of information security international standards to promote E-Publishing in Arab.

The researchers concluded in this paper many outcomes and the most significant one was international standards which have a crucial and important role in increasing the efficiency of E-Publishing over cloud computing via limiting the access to documents by (hackers, illegal access, unauthorized access and plagiarism) and enforces the role of control institutions to preserve researchers and authors copyright.

Researchers recommend using international standards on information security to enforce E-Publishing over cloud computing, addition to that it is set up an Arabic institute to issue information, standards which are compatible with the Arabic culture and environment.

Keywords- E-Publishing, Cloud Computing, Information Security Standards

I. INTRODUCTION

There is no doubt that information and communication revolution that the modern world faces have an impact and reflection on, institution’s management, natural assets, and services that it provides. Especially, after the huge immigration which information social faces in the 1990s the rapid growth of information and communication technology that gave the world a merge of computer techniques and long distance communications, a rise of developed networks and all the subsidiaries of E-Publishing.

All the mentioned above has a significant effect on gathering information broadly, therefore it achieved a crucial role of returning back the academic structure which is accredited by academic institutions and deliver it to the consumers, E-Publishing has made a great change in various technical and administrative procedures and especially E-Publishing over cloud computing. More than that many institutions were following this developed event and issue standards, rules, and principles to deal with and dump all the risks.

II. E-PUBLISHING

E-publishing is not a recent or new concept it has been mentioned and discussed in the previous century, but a rapid growth and development of the concept have been made in the 1990s; this development was because of the technical improvements and evolution of networks (E-system).

According to (Le Coadic, 1994) E-Publishing can be defined as “one of the most topics that will develop in future and it will be used broadly to publish articles swiftly, ease of access to them and a perfect way for research methods”[1].

(Bloor, 2000) mentioned that E-Publishing is a term initiated to cover a set of various information techniques and communications to be used for transferring a book content over networks (E-system) or mobile storage devices[2].

E-Publishing was defined by (Vickers and Martyn, 1994) as an application that requires from users to use electronic devices for receiving a document or a book content[3].

Where (Chennupati et al., 2006) defined this term as computer application prepared by the author to contain data and information for a specific sample of people and distribute it via information and communication techniques[4], where E-Publishing is a complete process aims to provide different types of information for a variant sample of users.

E-Publishing is classified according to (Deschamps, 1994) as following[5]:

- E-Books
- E-Courses
- E-Conferences
- Discussion lists
- Information bulletins

Therefore, E-Publishing can be defined as “the ability to access documents via World Wide Web (Internet) or mobile
storage devices which could not be as same as the hard copy; it contains same content with other facilities”.

(Saxena, 2009) assumed that E-Publishing is applied for the equation [6].

\[ \text{E-Publishing} = \text{E-System Techniques} + \text{Computer Techniques} + \text{Communication Techniques} + \text{Publish} \]

Where E-Publishing adds four terms together which is shown as well in figure (1):

**E-System Techniques** which intended of all techniques that provides capital and effort to increase the capital; **computer techniques** it means using computer to simplify work, take advantage of processor speed in processing data, storage capacity and employee it to work; **communication techniques** it's intended to employee the qualifications of communication networks in transferring information & Data; **Publish** such as editing, composition and promotion.

![Figure 1. The Components of E-Publishing](image)

Traditional publishing and E-Publishing doesn’t differ only in two phases as following [7]:

1. It doesn’t include using real materials such as ink and papers to print the final outcome.
2. There is no hard copy distribution for the publishers.

That mentioned above is because the final outcome must be electronic (digital) and intangible, therefore the outcome can be read over World Wide Web (Internet) through the use of computers, tablets, and smartphones and it could be printed as the United States of America according to the desire of the customer.

### III. E-PUBLISHING OVER CLOUD COMPUTING

The meaning of E-Publishing over cloud computing is that book content, and electronic documents which contain information and data will be published using storage capabilities of world wide web.

Therefore, the documents will be available to everyone who has the cost authorized access to download it which will ease the access, reduce cost and time.

There is a number of publishing security issues within cloud computing, where they comprehensive many techniques like; communication networks, database, operating systems, virtual simulation, resource scheduling, coefficients management, synchronization monitoring and storage management, all these made cloud computing security one of the most necessary conditions to achieve E-Publishing process successfully. For this all hardware equipment, must be set in a safe and secure location, data encryption, consider suitable policies with a national agreement to use international standards on information security for exchanging data and providing appropriate software to detect and delete malware programs [8].

#### A. The pros and cons of electronic publishing over cloud computing

There are many advantages the can be extracted from E-Publishing over cloud computing [9]:

1. Rapid access to the required document.
2. Reduction of publishing cost and storage cost.
3. Deliver contents that cannot be provided by mobile storage devices due to the size of data such as HD video clips.

On the other hand, there are some disadvantages that effected using by all countries and societies, as mentioned below [10]:

1. The issue of Internet speed download and upload and its availability especially in the outgrowth countries.
2. Cost of used devices to read electronic documents such as a laptop, tablet and smartphone has been increased.
3. Intellectual property rights (IPRs) are the most dangerous problems on E-Publishing over cloud computing, where most of the applied legislations in various countries could not ensure the protection of author’s rights in front of hackers and plagiarism.

#### B. Security Requirements for E-Publishing over Cloud Computing

To secure the E-Publishing over cloud computing process there is a must to provide the following [8]:
1. Support data storage efficiently and use encryption algorithms on data.
2. Manage & store huge amount of data via high-security cloud software.
3. Set security criteria to control the rank of authorization.
4. Applying international standards of information security in active and efficient manner.

IV. INFORMATION SECURITY

Many information security (InfoSec) organizations set a definition for this topic, as mentioned below[13]:

1. According to ISO, they defined (InfoSec) as; preserve information confidentiality and integrity with the ease of access to information, it also provides authenticity, accountability and reliability.
2. CNSS organization definition was; protecting information and information system from unauthorized access and editing on data, it also provides authenticity and integrity.
3. Where ISACA organization definition is: the insurance that only authorized user can gain and deal with detailed information confidentially and integrity.

On the other hand, many researchers and authors defined (InfoSec) as "process of preserving (IPRs) of the organization"[12], or "a confirmation that information is secured and risks are managed"[13].

(InfoSec) can be defined generally as "a region of various specialties for study workshop activities on security mechanisms developments to preserve information everywhere, protect its storage and mobility from threats"[11].

A. International standards of information security:

In order to insurance information trading generally whether electronically or hardcopy, many organizations issued standards, regulations, and rules, related to information security. The most important standards are listed below[14], [15].

1. ISO Standards; ISO is known as an international organization for standard unification, it was established in 1947 where it’s a non-governmental institute that corporate with electronic technique committee (IEC) and international union of communication (ITU), mentioned below is the information security standards related to this organization:
   - ISO 27001: this standard introduces a periodic model (PDCA) which stands for (Plan-Do-Check-Act) and aims to determine the necessary needs to establish, execute, operate, exhibit, enhance and document information security management system.
   - ISO 27002: the standard includes some policies, security policy orientation; organize of information

security, human resource insurance, and assets management.
   - ISO 15408: this standard aids in evaluating, verify and certificate security insurance for technical products and also evaluate devices and software allocated to E-Publishing.
   - ISO 13335: consist of principles and directions serial to document concepts, modeling security of information and communication techniques management, select technical security controls and administration guidance for network security.
2. COBIT Standard; its considered as control framework that connects information techniques and work requirements and organizing information techniques activities in an information security process model, the standard was constructed by Governmental Information Techniques Institute (GITI) in 1995.
3. ITIL Standard; represents a set of best practices in information technique management (ITSM) and it focuses on the services of information techniques processes where it is the main role for users. It was issued by Office of the United Kingdom Trade Government (OGC).
4. Regulations and rules related to information security; there is many regulations, direction principles and rules, such as:
   - SOX Act: stands for Sarbanes-Oxley Act this rule raised in 2002 after the scandals of WorldCom and Enron firms, the purpose of issuing at the beginning was to improve disclosure accuracy and reliability in American financial market but later it became an Icon of information security through developing for interior monitoring of E-Publishing.
   - COSO Act: it stands for Committee of Sponsoring Organization of the Trade Way Commission and it’s a framework that starts from interior control and improves control means to deploy information electronically by environment monitoring and risk evaluation.
   - HIPAA Act: this term stands for The Health Insurance Portability and Accountability Act which is a rule dedicated in United States of America aims to enhance information security for Healthcare, set main regulations to protect information that threats safety and security of original information and detect unauthorized access to it.
   - FISMA Act: the term came from Federal Information Security Management Act, where it's used to manage federal information security and functions periodically as a risk evaluation for information and set strategies to provide security for networks, information systems and E-Publishing.
   - FIPS Act: stands for The Federal Information Processing Standards this means a standard to process
federal information, it’s considered as a set of official publishes related to accredited direction principles and standards for E-Publishing, auditing, certificate and urgent planning.

Figure (2) depicts the most significant international standards for information security which is used in E-Publishing information insurance in many countries.

![International Standards for Information Security](image.png)

Figure 2. International Standards for Information Security

V. EXPERIMENTAL SECTION (DATA ANALYSIS)

To measure an impact of international standards on information security to enhance the efficiency of E-Publishing over cloud computing, a questionnaire form was designed by researchers which consist of 4 axes (A, B, C, and D).

Where selecting, an axis is done through assists of research literature reviews, this axis includes 10 questions related to information security and E-Publishing where 100 questionnaire forms were distributed to academics and researchers of different specialties as shown in the table (1).

<table>
<thead>
<tr>
<th>S/N</th>
<th>Certificates Position</th>
<th>Orientation</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bachelor Practitioner</td>
<td>Technical</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>Bachelor Researcher</td>
<td>Academic</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Diploma Practitioner</td>
<td>Technical</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>M.Sc. Lecturer</td>
<td>Academic</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>Ph.D. Lecturer</td>
<td>Academic</td>
<td>20</td>
</tr>
</tbody>
</table>

Fuzzy logic tools have been used to analyze the results of gathered questionnaire form via applying it in MATLAB software to gain real results that aren’t subject to personal strain and according to sampler’s opinion.

A. Questionnaire Form Axes

Questionnaire form is categorized into (4) Axes to familiarity case study in a subjective manner, these Axes are:

1. The role of information security international standards to limit hacking and illegal copies problems.
   - A Axes: The purpose of this axis is to measure impact of applying international standards for information security to limit hacking and illegal copies, a significant ratio of (40%) is determined for (A) Axis and assign percentage weights for axis questions as shown in Table (2) according to sampler’s opinion then determine weight percentage for the Axis in all, this is depicted in Table (4) after that all processed outcomes are gathered via fuzzy logic tools as shown in Table (4).

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Ext. Disagree</th>
<th>Disagree</th>
<th>N.</th>
<th>Agree</th>
<th>Ext. Agree</th>
<th>Q. Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_1</td>
<td>0.625</td>
<td>0.25</td>
<td>1.375</td>
<td>0.35</td>
<td>2.75</td>
<td>1.1</td>
</tr>
<tr>
<td>A_2</td>
<td>0.4</td>
<td>0.16</td>
<td>0.6</td>
<td>0.24</td>
<td>2.3</td>
<td>0.92</td>
</tr>
<tr>
<td>A_3</td>
<td>0.7</td>
<td>0.28</td>
<td>0.7</td>
<td>0.28</td>
<td>2.3625</td>
<td>0.945</td>
</tr>
<tr>
<td>A_4</td>
<td>0.35</td>
<td>0.14</td>
<td>0</td>
<td>0</td>
<td>1.4</td>
<td>0.56</td>
</tr>
<tr>
<td>A_5</td>
<td>0.75</td>
<td>0.3</td>
<td>1.5</td>
<td>0.6</td>
<td>1</td>
<td>0.4</td>
</tr>
<tr>
<td>A_6</td>
<td>0.875</td>
<td>0.35</td>
<td>0.625</td>
<td>0.25</td>
<td>2.625</td>
<td>1.05</td>
</tr>
<tr>
<td>A_7</td>
<td>0.75</td>
<td>0.3</td>
<td>1.05</td>
<td>0.42</td>
<td>1.05</td>
<td>0.42</td>
</tr>
<tr>
<td>A_8</td>
<td>0.3</td>
<td>0.12</td>
<td>0.4</td>
<td>0.16</td>
<td>0.4</td>
<td>0.16</td>
</tr>
<tr>
<td>A_9</td>
<td>0.225</td>
<td>0.09</td>
<td>0.675</td>
<td>0.27</td>
<td>0.3</td>
<td>0.12</td>
</tr>
<tr>
<td>A_10</td>
<td>0.15</td>
<td>0.06</td>
<td>0.375</td>
<td>0.15</td>
<td>1.5</td>
<td>0.6</td>
</tr>
</tbody>
</table>

Table 3: Measure of Ratio Weights for Questionnaire According to Axis and Form in all
Table 4: Measure of Compatibility About the Axis

<table>
<thead>
<tr>
<th>Acceptance Degree</th>
<th>Axis Impact</th>
<th>Questionnaire Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Disagree</td>
<td>5.125</td>
<td>2.05</td>
</tr>
<tr>
<td>Disagree</td>
<td>7.3</td>
<td>2.92</td>
</tr>
<tr>
<td>Neutral</td>
<td>15.6875</td>
<td>6.275</td>
</tr>
<tr>
<td>Agree</td>
<td>41.7</td>
<td>16.68</td>
</tr>
<tr>
<td>Extremely Agree</td>
<td>30.1875</td>
<td>12.075</td>
</tr>
</tbody>
</table>

2. The role of information security international standards on preserving publishes rights for researchers and authors.

- **B Axes**: The purpose of this axis is to measure an impact of applying international standards for information security to preserve publishing rights. Therefore, a significant ratio of (30%) is determined for (B) Axis and assign percentage weights for axis questions as shown in Table (5) according to sampler’s opinion then determine weight percentage for the Axis in all, this is depicted in Table (6) after that all processed outcomes are gathered by using fuzzy logic tools as shown in Table (7).

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Ext. Disagree</th>
<th>Disagree</th>
<th>N. Agree</th>
<th>Ext. Agree</th>
<th>Q. Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>7</td>
<td>16</td>
<td>20</td>
<td>36</td>
<td>26</td>
</tr>
<tr>
<td>B2</td>
<td>5</td>
<td>8</td>
<td>18</td>
<td>37</td>
<td>32</td>
</tr>
<tr>
<td>B3</td>
<td>7</td>
<td>16</td>
<td>25</td>
<td>25</td>
<td>37</td>
</tr>
<tr>
<td>B4</td>
<td>15</td>
<td>7</td>
<td>16</td>
<td>25</td>
<td>37</td>
</tr>
<tr>
<td>B5</td>
<td>12</td>
<td>11</td>
<td>18</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>B6</td>
<td>11</td>
<td>6</td>
<td>18</td>
<td>25</td>
<td>33</td>
</tr>
<tr>
<td>B7</td>
<td>3</td>
<td>9</td>
<td>19</td>
<td>41</td>
<td>28</td>
</tr>
<tr>
<td>B8</td>
<td>12</td>
<td>13</td>
<td>22</td>
<td>36</td>
<td>24</td>
</tr>
<tr>
<td>B9</td>
<td>13</td>
<td>11</td>
<td>18</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>B10</td>
<td>6</td>
<td>10</td>
<td>11</td>
<td>37</td>
<td>36</td>
</tr>
</tbody>
</table>

Table 6: Measure of Ratio Weights for Questionnaire According to Axis and Form in all

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Ext. Disagree</th>
<th>Disagree</th>
<th>Natural</th>
<th>Agree</th>
<th>Extremely Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>0.7</td>
<td>0.21</td>
<td>1.6</td>
<td>0.48</td>
<td>2.625</td>
</tr>
<tr>
<td>B2</td>
<td>1.125</td>
<td>0.3375</td>
<td>1.2</td>
<td>0.36</td>
<td>2.625</td>
</tr>
<tr>
<td>B3</td>
<td>0.75</td>
<td>0.225</td>
<td>1.6</td>
<td>0.48</td>
<td>2.625</td>
</tr>
<tr>
<td>B4</td>
<td>0.7</td>
<td>0.21</td>
<td>0.9</td>
<td>0.27</td>
<td>2.625</td>
</tr>
<tr>
<td>B5</td>
<td>0.75</td>
<td>0.225</td>
<td>1.25</td>
<td>0.375</td>
<td>2.625</td>
</tr>
<tr>
<td>B6</td>
<td>1.65</td>
<td>0.495</td>
<td>0.9</td>
<td>0.27</td>
<td>2.625</td>
</tr>
<tr>
<td>B7</td>
<td>1.125</td>
<td>0.3375</td>
<td>0.525</td>
<td>0.1575</td>
<td>2.625</td>
</tr>
<tr>
<td>B8</td>
<td>0.6</td>
<td>0.18</td>
<td>0.55</td>
<td>0.165</td>
<td>2.625</td>
</tr>
<tr>
<td>B9</td>
<td>0.15</td>
<td>0.045</td>
<td>0.45</td>
<td>0.135</td>
<td>2.625</td>
</tr>
<tr>
<td>B10</td>
<td>0.375</td>
<td>0.1125</td>
<td>0.975</td>
<td>0.2925</td>
<td>2.625</td>
</tr>
</tbody>
</table>

Table 7: Measure of Compatibility About the Axis

<table>
<thead>
<tr>
<th>Acceptance Degree</th>
<th>Axis Impact</th>
<th>Questionnaire Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Disagree</td>
<td>7.925</td>
<td>2.3775</td>
</tr>
<tr>
<td>Disagree</td>
<td>8.75</td>
<td>2.625</td>
</tr>
<tr>
<td>Neutral</td>
<td>18.75</td>
<td>5.625</td>
</tr>
<tr>
<td>Agree</td>
<td>33.8</td>
<td>10.14</td>
</tr>
<tr>
<td>Extremely Agree</td>
<td>30.775</td>
<td>9.2325</td>
</tr>
</tbody>
</table>

3. The role of information security international standards to reduce the cost of electronic storage.

- **C Axes**: The purpose of this axis is to measure an impact of applying international standards for information security to reduce the cost of electronic storage. Therefore, a significant ratio of (20%) is determined for (C) Axis and assign percentage weights for axis questions as shown in Table (8) according to sampler’s opinion then determine weight percentage for the Axis in all, this is depicted in Table (9) after that all processed outcomes are gathered by using fuzzy logic tools as shown in Table (10).

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Ext. Disagree</th>
<th>Disagree</th>
<th>N. Agree</th>
<th>Ext. Agree</th>
<th>Q. Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>19</td>
<td>14</td>
<td>15</td>
<td>28</td>
<td>24</td>
</tr>
<tr>
<td>C2</td>
<td>12</td>
<td>18</td>
<td>19</td>
<td>28</td>
<td>30</td>
</tr>
<tr>
<td>C3</td>
<td>17</td>
<td>20</td>
<td>14</td>
<td>27</td>
<td>22</td>
</tr>
<tr>
<td>C4</td>
<td>13</td>
<td>11</td>
<td>12</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>C5</td>
<td>11</td>
<td>15</td>
<td>13</td>
<td>28</td>
<td>33</td>
</tr>
<tr>
<td>C6</td>
<td>15</td>
<td>19</td>
<td>17</td>
<td>15</td>
<td>34</td>
</tr>
<tr>
<td>C7</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>30</td>
</tr>
<tr>
<td>C8</td>
<td>12</td>
<td>14</td>
<td>19</td>
<td>28</td>
<td>30</td>
</tr>
<tr>
<td>C9</td>
<td>10</td>
<td>19</td>
<td>22</td>
<td>29</td>
<td>20</td>
</tr>
<tr>
<td>C10</td>
<td>11</td>
<td>12</td>
<td>20</td>
<td>30</td>
<td>27</td>
</tr>
</tbody>
</table>
Table 9: Measure of Ratio Weights for Questionnaire According to Axis and Form in all

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Extremely Disagree</th>
<th>Disagree</th>
<th>Natural</th>
<th>Agree</th>
<th>Extremely Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Axis</td>
<td>Form</td>
<td>Axis</td>
<td>Form</td>
<td>Axis</td>
</tr>
<tr>
<td>C_1</td>
<td>2.137</td>
<td>0.4275</td>
<td>1.575</td>
<td>0.315</td>
<td>1.6875</td>
</tr>
<tr>
<td>C_2</td>
<td>1.2</td>
<td>0.24</td>
<td>1.8</td>
<td>0.36</td>
<td>1.9</td>
</tr>
<tr>
<td>C_3</td>
<td>1.7</td>
<td>0.34</td>
<td>2</td>
<td>0.4</td>
<td>1.4</td>
</tr>
<tr>
<td>C_4</td>
<td>1.625</td>
<td>0.325</td>
<td>1.375</td>
<td>0.275</td>
<td>1.5</td>
</tr>
<tr>
<td>C_5</td>
<td>0.667</td>
<td>0.1375</td>
<td>0.9375</td>
<td>0.1875</td>
<td>0.8125</td>
</tr>
<tr>
<td>C_6</td>
<td>1.5</td>
<td>0.3</td>
<td>1.9</td>
<td>0.38</td>
<td>1.7</td>
</tr>
<tr>
<td>C_7</td>
<td>2.4</td>
<td>0.48</td>
<td>2.55</td>
<td>0.51</td>
<td>2.7</td>
</tr>
<tr>
<td>C_8</td>
<td>0.9</td>
<td>0.18</td>
<td>0.825</td>
<td>0.165</td>
<td>1.425</td>
</tr>
<tr>
<td>C_9</td>
<td>0.75</td>
<td>0.15</td>
<td>1.425</td>
<td>0.285</td>
<td>1.65</td>
</tr>
<tr>
<td>C_10</td>
<td>1.1</td>
<td>0.22</td>
<td>1.2</td>
<td>0.24</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 10: Measure of Compatibility About the Axis

<table>
<thead>
<tr>
<th>Acceptance Degree</th>
<th>Axis Impact</th>
<th>Questionnaire Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Disagree</td>
<td>14</td>
<td>2.8</td>
</tr>
<tr>
<td>Disagree</td>
<td>15.5875</td>
<td>3.1175</td>
</tr>
<tr>
<td>Neutral</td>
<td>16.775</td>
<td>3.355</td>
</tr>
<tr>
<td>Agree</td>
<td>25.2</td>
<td>5.04</td>
</tr>
<tr>
<td>Extremely Agree</td>
<td>28.4375</td>
<td>5.6875</td>
</tr>
</tbody>
</table>

4. The role of information security international standards on quick access to the desired goal.

- D Axes: The purpose of this axis is to measure an impact of applying international standards for information security on quick access to the desired goal. Therefore, a significant ratio of (10%) is determined for (D) Axis and assign percentage weights for axis questions as shown in Table (11) according to sampler’s opinion then determine weight percentage for the axis in all, this is depicted in Table (12) after that all processed outcomes are gathered by using fuzzy logic tools as shown in Table (13).

Table 11: Sampler’s Opinion about (D) Axis

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Ext. Disagree</th>
<th>Disagree</th>
<th>N.</th>
<th>Agree</th>
<th>Ext. Agree</th>
<th>Q. Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>D_1</td>
<td>24</td>
<td>25</td>
<td>21</td>
<td>20</td>
<td>10</td>
<td>0.125</td>
</tr>
<tr>
<td>D_2</td>
<td>18</td>
<td>23</td>
<td>22</td>
<td>24</td>
<td>13</td>
<td>0.1</td>
</tr>
<tr>
<td>D_3</td>
<td>25</td>
<td>24</td>
<td>18</td>
<td>27</td>
<td>6</td>
<td>0.075</td>
</tr>
<tr>
<td>D_4</td>
<td>21</td>
<td>26</td>
<td>19</td>
<td>13</td>
<td>21</td>
<td>0.125</td>
</tr>
<tr>
<td>D_5</td>
<td>19</td>
<td>21</td>
<td>17</td>
<td>20</td>
<td>23</td>
<td>0.075</td>
</tr>
<tr>
<td>D_6</td>
<td>23</td>
<td>16</td>
<td>23</td>
<td>15</td>
<td>23</td>
<td>0.075</td>
</tr>
<tr>
<td>D_7</td>
<td>25</td>
<td>19</td>
<td>19</td>
<td>15</td>
<td>22</td>
<td>0.015</td>
</tr>
<tr>
<td>D_8</td>
<td>20</td>
<td>18</td>
<td>21</td>
<td>23</td>
<td>18</td>
<td>0.125</td>
</tr>
<tr>
<td>D_9</td>
<td>23</td>
<td>20</td>
<td>20</td>
<td>21</td>
<td>16</td>
<td>0.11</td>
</tr>
<tr>
<td>D_10</td>
<td>15</td>
<td>23</td>
<td>21</td>
<td>20</td>
<td>21</td>
<td>0.175</td>
</tr>
</tbody>
</table>

Table 12: Measure of Ratio Weights for Questionnaire According to Axis and Form in all

<table>
<thead>
<tr>
<th>Q. Code</th>
<th>Extremely Disagree</th>
<th>Disagree</th>
<th>Natural</th>
<th>Agree</th>
<th>Extremely Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Axis</td>
<td>Form</td>
<td>Axis</td>
<td>Form</td>
<td>Axis</td>
</tr>
<tr>
<td>D_1</td>
<td>3</td>
<td>0.3</td>
<td>3.125</td>
<td>0.3125</td>
<td>2.625</td>
</tr>
<tr>
<td>D_2</td>
<td>1.8</td>
<td>0.18</td>
<td>2.3</td>
<td>0.23</td>
<td>2.2</td>
</tr>
<tr>
<td>D_3</td>
<td>1.875</td>
<td>0.1875</td>
<td>1.8</td>
<td>0.18</td>
<td>1.35</td>
</tr>
<tr>
<td>D_4</td>
<td>2.625</td>
<td>0.2625</td>
<td>3.25</td>
<td>0.325</td>
<td>2.375</td>
</tr>
<tr>
<td>D_5</td>
<td>1.425</td>
<td>0.1425</td>
<td>1.575</td>
<td>0.1575</td>
<td>1.275</td>
</tr>
<tr>
<td>D_6</td>
<td>1.725</td>
<td>0.1725</td>
<td>1.2</td>
<td>0.12</td>
<td>1.725</td>
</tr>
<tr>
<td>D_7</td>
<td>0.375</td>
<td>0.0375</td>
<td>0.285</td>
<td>0.0285</td>
<td>0.265</td>
</tr>
<tr>
<td>D_8</td>
<td>2.5</td>
<td>0.25</td>
<td>2.25</td>
<td>0.225</td>
<td>2.625</td>
</tr>
<tr>
<td>D_9</td>
<td>2.53</td>
<td>0.253</td>
<td>2.2</td>
<td>0.22</td>
<td>2.2</td>
</tr>
<tr>
<td>D_10</td>
<td>2.625</td>
<td>0.2625</td>
<td>4.025</td>
<td>0.4025</td>
<td>3.675</td>
</tr>
</tbody>
</table>

Table 13: Measure of Compatibility About the Axis

<table>
<thead>
<tr>
<th>Acceptance Degree</th>
<th>Axis Impact</th>
<th>Questionnaire Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Disagree</td>
<td>20.48</td>
<td>2.048</td>
</tr>
<tr>
<td>Disagree</td>
<td>22.01</td>
<td>2.2</td>
</tr>
<tr>
<td>Neutral</td>
<td>20.335</td>
<td>2.0335</td>
</tr>
<tr>
<td>Agree</td>
<td>20.085</td>
<td>2.0085</td>
</tr>
<tr>
<td>Extremely Agree</td>
<td>17.09</td>
<td>1.709</td>
</tr>
</tbody>
</table>

All the Axes which have been analyzed by measuring the effect of applying international standards for information security to improve the efficiency of E-Publishing were selected because of its cohesion with information security international standards.

In the return to above tables, an impact could be determined for information security international standards to enhance the efficiency of E-Publishing over cloud computing according to sampler’s opinion, using fuzzy logic tools as shown in Table (14).
Table (14) Determine the impact of information security international standards to enhance the efficiency of E-Publishing over cloud computing

<table>
<thead>
<tr>
<th>Degree</th>
<th>A Axis</th>
<th>B Axis</th>
<th>C Axis</th>
<th>D Axis</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Disagree</td>
<td>2.05</td>
<td>2.3775</td>
<td>2.8</td>
<td>2.048</td>
<td>9.2755</td>
</tr>
<tr>
<td>Disagree</td>
<td>2.92</td>
<td>2.625</td>
<td>3.1175</td>
<td>2.201</td>
<td>10.8635</td>
</tr>
<tr>
<td>Neutral</td>
<td>6.275</td>
<td>5.625</td>
<td>3.355</td>
<td>2.0335</td>
<td>20.139</td>
</tr>
<tr>
<td>Agree</td>
<td>16.68</td>
<td>10.14</td>
<td>5.04</td>
<td>2.0085</td>
<td>33.8685</td>
</tr>
<tr>
<td>Extremely Agree</td>
<td>12.075</td>
<td>9.2325</td>
<td>5.6875</td>
<td>1.709</td>
<td>28.704</td>
</tr>
</tbody>
</table>

CONCLUSIONS

Researchers have concluded the following results:

- Information Security International Standards effects on the Efficiency of E-Publishing through the limitation of unauthorized copies and hacking, where the results of analyzing questionnaire show that (71%) agrees while (21%) doesn’t agree.

- Information Security International Standards can increase security factor for researchers and authors rights where (64%) agreed that there is an effect while (16%) refused.

- Information Security International Standards has an impact on electronic storage costs, results showed that (54%) agree and (30%) don’t agree.

- Quick access to the desired goal or document has a relationship with Information Security International Standards, where outcomes showed that (37%) agrees and (42%) doesn’t agree.

- Generally, the final results of analyzing questionnaire form proved that (63%) of researchers and academics confirmed there is a robust relationship between Information Security International Standards and the increase of E-Publishing over cloud computing efficiency.

RECOMMENDATIONS

- On the basis of results mentioned earlier, the researchers recommend the following:
  - To promote the E-Publishing over cloud computing it’s a must to use Information Security International Standards.
  - Develop an Arabic institute to issue Information Security International Standards which it goes with the environment and Arabic culture.
  - Increase the culture conscious for researchers and academics about Information Security International Standards and its effect on E-Publishing and traditional publishing.

REFERENCES

PerfectC^2MIS: A perfect FileMaker r-database based comprehensive Class cum Course Management Information System

Atul Sharma
Department of Banking & Financial Sciences
Cihan University, Erbil
atul.sharma@cihanuniversity.edu.iq

Omead Ibraheem Hussain
Department of Banking & Financial Sciences
Cihan University, Erbil
omead.h@cihanuniversity.edu.iq

Abstract-As most of us are unaware that we have a very effective and efficient relational database with the name FileMaker which falls under the category of less known Relational Database Management System (RDBMS) to develop and deploy all types of computer applications to manage the business of a Small and Medium Enterprises (SME’s). Our research paper presents a time tested computerized information system designed to manage class/department for Cihan University, Erbil. The main objective of this research paper is to offer an automated, faster and efficient system to the end-user in order to process faster and increase the overall efficiency in the overall cycle. As of now the system has been deployed for single entity i.e. teacher. Later on we would extend it to the usage of Head of the Department (HOD) & the office secretary as well. Our objective of this practical research would be to focus on the design part as well as the functionality of the application software.

Keywords: RDBMS, ICT, Information Technology

1. INTRODUCTION

These days the database has become one of the most important tools for storing, analyzing complex information and large amount of data as per the figure 1 below:-

A well designed database structure has several plus points like fast, accurate, real-time access, perfect reporting, highly scalable, and error free etc. It is one of the most common tools in business houses, banks, government, industries, and schools, colleges globally to process the data & use the processed information as a result.

Information technologies are the result of knowledge explosion. These include hardware & software technologies and facilitate teaching learning process. Using Information Technologies learners are now able to participate in learning communities throughout the world. They are independent and free in choice of their programmes of study and access to the resources. They may learn collaboratively, share information, exchange their learning experiences and work through cooperative activities in virtual learning communities [2].

![Figure 1- The data-information cycle](image-url)
knowledge as per the data-information cycle shown in Figure 1 above. As a result these schools have been able to perform overall much better than those without it. A typical Class Management System is the usage of a large database comprising of smaller table spaces which can be used to manage any class perfectly well. It consists of recording & retrieval of all the activities of students on day to day basis. This information is extremely useful at time like Parent Teacher Meeting (PTM) etc. We can have a standalone system or a multiuser system that can be accessed by many users at the same time. In other words we can say that our application is a supporting tool which can be accessed in one of the many ways like –

- Standalone
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Web

This paper deals with the development and deployment of such Information Technology (IT) based Management Information System at Cihan University, Erbil.

2. MOTIVATION

Further, this processed information can be conveniently accessed & shared with the authorized users at any point of time. This type of user access control program has been projected for a future release. Everything becomes so easy to process & prepare the flexible management information system reports in a fraction of second with the press of a button.

Actually Cihan University is working on an action plan which aims at a maximum usage of Information & Communication Technology (ICT) in almost all the operations at all the levels. Information and communication technologies (ICTs) are a group of technologies and tools which, at one hand are useful for learners by facilitating them with global access, library services and communication with experts, resource persons, researcher, professionals, and peers; on the other hand important for teachers in course design, developing course materials and in research. ICTs are important in distance education due to their potential in teaching-learning, to increase flexibility of learning with tools like Virtual Learning Environments, and Course Management Systems like Moodle, aTutor, online discussion boards, wikis, chat rooms, MOOCs and blogs. The major advantages of using technologies in distance education are cost effectiveness, time saving, improved quality of education, access to a larger population, teaching a no. of students simultaneously, and finding a lot of educational resources [3]. Therefore, their needs moved towards Class Management Systems (CMS) as a best fit solution for managing any data related to students, employees, teaching processes etc. Such an automated system can make life peaceful and easier for any end user. Using PerfectC^2MIS, finding student’s information is fast and fluid which otherwise could have taken a much longer duration. At the end of each semester, printing students’ overall performance statement including attendance, grades, notes becomes just a few seconds job which otherwise could have taken a much longer time without using our application.

With the initiative of the management of the Cihan Educational Group and the whole hearted support of the concerned departments a project team was formed for the design and implementation of the automated system. The primary objective of our project was to develop an automated computer based system for Cihan University to computerize all the teaching procedures &
practices being followed in the management of the classes conducted at Cihan University.

3. SYSTEM DEVELOPMENT

PerfectC²MIS is being used at a standalone system at the present time. Later on we would migrate our application to Client-Server environment. Client-Server computing uses local processing power-the power of desktop platform. It changes the way enterprise accesses, distributes, and uses data. With this approach, data is no longer under the tight control of Seniors Managers and MIS (Management of Information Systems) staff; it is readily available to middle-rank personnel and staff. They can actively involve in the decision-making and operation on behalf of the company. The company becomes more flexible and gives a faster response to the changing business environment outside. In addition, if one machine goes down, the company will still function properly [5]. At the present time we can execute our application on a standalone module although the same application has been tested to work on Local Area Network (LAN) as well. In this scenario we have just one drawback that our database cannot be centralized. All the users are unable to share the information between them. Later on with the purchase of server edition of FileMaker we would be able to map it to the server edition as well. Further we have very efficient & fast file servers at the backend to manage the show. Our application should be hardware and software independent as well. Figure 2 below shows the screenshot of the main screen of the application PerfectC²MIS.

3.1 Analysis and Definition

A detailed session of discussions and meetings was carried out with the potential users of the system as well as concerned staff. Based on these inputs a detailed SRS (System Requirement Specifications) document was prepared. This consisted of existing hardcopies of forms and reports served as a good reference for the best possible solution of the final SRS. Paper documentation serves as a rich input to understand the existing procedures/activities performed within the department. Failure projects are those ones that do not meet the original time, cost and quality requirements criteria. The common cause of software project failure: absence of well-defined requirements.

Figure 2 - Screenshot of the main screen of PerfectC²MIS
With some hardships we were able to understand the required system from the end user as well as the cooperation from the administrative staff. All the inputs were collected with just point in the mind that was to streamline the system to the maximum. Figure 3 above shows the User-case Diagram for one user i.e. the teacher. Later on we would work on to release updated modules for:

- Head of the Department
- Secretary
- Students

It has been found that the end users are not fully versed with the complete requirements of the system. Henceforth it becomes very important for the analyst to understand the complete System Requirement Specifications (SRS) with the designated in charge. The output of the requirements phase of the software development process is Software Requirements Specification (SRS) (also known as requirements document). This document lays a foundation for software engineering activities and is created when entire requirements are elicited and analyzed. SRS is a formal document, which acts as a representation of software that enables the users to review whether it (SRS) is according to their requirements. In addition, it includes user requirements for a system as well as detailed specifications of the system requirements [4]. Initially we face some resistance from the end users in using the system but later on they would be able to accept it. Further we also need to note that if our application does not help and facilitate the user’s work they will be reluctant to use it. We need handle such situations tactfully.

3.2 Software Design

As we all know that software design is the most critical element of any project. The success of any project lies in the quality of software design. Software Design is the study of the modern methods, technologies, languages, principles and practices that make it possible to conceive, create, validate and evolve complex software systems [1]. It consists of understanding user requirements completely & correctly. Further we need to complete the paperwork like SRS, DFD’s, and ERD’s as well. Making a complete sketch of Data tables & their fields is again a very important part of software design.

3.2.1 Data Model

The first step in the data modeling module is defining a good consistent structured database. This model of our project is represented by the data model which
CIC-COCOS’17

March 29-30, 2017, Cihan University-Erbil

consists of various entities as shown in figures below:-

The figure 4 shows a typical Table space in the FileMaker. Like this we have other database structures as well. We just need to link them together as per our requirement.

![Figure 4: A typical Table space](image)

During the designing of the database, we need to make right decisions to make the best use of an effective and efficient system. A well worked on database takes less time and efforts to process and produce end results. For the reason a lot of the success of the project depends on the designing of the data model. It should be scalable with the options to modify as and when required. It should be easy to understand & user-friendly. We need to take care of data redundancy. Further our application should be flexible so that it can be used anywhere with no hardware or software limitations and should work perfectly well with changing requirements with minimum efforts.

In figure 6 above we show the most important entities of the model and their relationships as defined & used in a typical class/session in our Cihan University. Our whole project is usually based on this ER diagram (Entity-relationship) diagrams.

![Figure 5: A typical FileMaker Table structure](image)

![Figure 6: A typical Entity-Relationship diagram in FileMaker](image)
3.3 Implementation

The next step is the implementation of the application software which has been developed as a constructive effort of the entire team. The communication between the database and the software includes:

- Storing data/information in the database
- Modifying data/information as and when required
- Retrieving the required data/information as required

4. CONCLUSIONS

The need of managing the information electronically has been growing manifold in all areas of the Kurdistan region. As we all know that education is considered to be very essential for the development of any nation. Therefore, Class Management Systems like PerfectC²MIS have been suggested as the best option to manage information in the schools/colleges.

The PerfectC²MIS application software has been built based on actual procedures and practices being followed in Cihan University. Therefore, this system may be considered as a very critical step aimed towards implementing digitally based information management in Schools/Universities.

5. ACKNOWLEDGEMENT

This research has been highly supported by Cihan Educational Group. We thank our colleagues from Cihan University who provided valuable inputs for the success of the project.

6. REFERENCES


