http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 5 Issue 5, Sep. 2016, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI Global IT Research Institute

Journal Editorial Board

■ Editor-in-Chief

■ Editors

Dr. Youssef SAID, Tunisie Telecom, Tunisia
Dr. Noor Zaman, King Faisal University, Al Ahsa Hofuf, Saudi Arabia
Dr. Srinivas Mantha, SASTRA University, Thanjavur, India
Dr. Shahriar Mohammadi, KNTU University, Iran
Prof. Beonsku An, Hongik University, korea
Dr. Guanbo Zheng, University of Houston, USA
Prof. Sangho Choe, The Catholic University of Korea, korea
Dr. Gyanendra Prasad Joshi, Yeungnam University, korea
Dr. Tae-Gyu Lee, Korea Institue of Industrial Technology(KITECH), korea
Prof. Ilkyeun Ra, University of Colorado Denver, USA
Dr. Yong Sun, Beijing University of Posts and Telecommunications, China
Dr. Yulei Wu, Chinese Academy of Sciences, China
Mr. Anup Thapa, Chosun University, korea
Dr. Vo Nguyen Quoc Bao, Posts and Telecommunications Institute of Technology, Vietnam
Dr. Harish Kumar, Bhagwant institute of technology, India
Dr. Jin REN, North china university of technology, China
Dr. Joseph Kandath, Electronics & Commn Engg, India
Dr. Mohamed M. A. Moustafa, Arab Information Union (AIU), Egypt
Dr. Mostafa Zaman Chowdhury, Kookmin University, Korea
Prof. Francis C.M. Lau, Hong Kong Polytechnic University, Hong Kong
Prof. Ju Bin Song, Kyung Hee University, korea
Prof. KyungHi Chang, Inha University, Korea
Prof. Sherif Welsen Shaker, Kuang-Chi Institute of Advanced Technology, China
Prof. Seung-Hoon Hwang, Dongguk University, Korea
Prof. Dal-Hwan Yoon, Semyung University, korea
Prof. Chongyang ZHANG, Shanghai Jiao Tong University, China
Dr. H K Lau, The Open University of Hong Kong, Honh Kong
Prof. Ying-Ren Chien, Department of Electrical Engineering, National Ilan University, Taiwan
Prof. Mai Yi-Ting, Hsiuping University of Science and Technology, Taiwan
Dr. Sang-Hwan Ryu, Korea Railroad Research Institute, Korea
Dr. Yung-Chien Shih, MediaTek Inc., Taiwan
Dr. Kuan Hoong Poo, Multimedia University, Malaysia
Dr. Michael Leung, CEng MIET SMIEEE, Hong Kong
Dr. Abu sahman Bin mohd Supa'at, Universiti Teknologi Malaysia, Malaysia
Prof. Amit Kumar Garg, Deenbandhu Chhotu Ram University of Science & Technology, India
Dr. Jens Myrup Pedersen, Aalborg University, Denmark
Dr. Augustine Ikechi Ukaegbu, KAIST, Korea
Dr. Jamshid Sangirov, KAIST, Korea
Prof. Ahmed Dooguy KORA, Ecole Sup. Multinationale des Telecommunications, Senegal
Dr. Se-Jin Oh, Korea Astronomy & Space Science Institute, Korea
Dr. Rajendra Prasad Mahajan, RGPV Bhopal, India
Dr. Woo-Jin Byun, ETRI, Korea
Dr. Mohammed M. Kadhum, School of Computing, Goodwin Hall, Queen's University , Canada
Prof. Seong Gon Choi, Chungbuk National University, Korea
Prof. Yao-Chung Chang, National Taitung University, Taiwan
Dr. Abdallah Handoura, Engineering school of Gabes - Tunisia, Tunisia
Dr. Gopal Chandra Manna, BSNL, India

Dr. Il Kwon Cho, National Information Society Agency, Korea
Prof. Jiann-Liang Chen, National Taiwan University of Science and Technology, Taiwan
Prof. Ruay-Shiung Chang, National Dong Hwa University, Taiwan
Dr. Vasaka Visoottiviseth, Mahidol University, Thailand
Prof. Dae-Ki Kang, Dongseo University, Korea
Dr. Yong-Sik Choi, Research Institute, IDLE co., ltd, Korea
Dr. Xuena Peng, Northeastern University, China
Dr. Ming-Shen Jian, National Formosa University, Taiwan
Dr. Soobin Lee, KAIST Institute for IT Convergence, Korea
Prof. Yongpan Liu, Tsinghua University, China
Prof. Chih-Lin HU, National Central University, Taiwan
Prof. Chen-Shie Ho, Oriental Institute of Technology, Taiwan
Dr. Hyoung-Jun Kim, ETRI, Korea
Prof. Bernard Cousin, IRISA/Universite de Rennes 1, France
Prof. Eun-young Lee, Dongduk Woman s University, Korea
Dr. Porkumaran K, NGP institute of technology India, India
Dr. Feng CHENG, Hasso Plattner Institute at University of Potsdam, Germany
Prof. El-Sayed M. El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Prof. Lin You, Hangzhou Dianzi Univ, China
Mr. Nicolai Kuntze, Fraunhofer Institute for Secure Information Technology, Germany
Dr. Min-Hong Yun, ETRI, Korea
Dr. Seong Joon Lee, Korea Electrotechnology Research Institute, korea
Dr. Kwihoon Kim, ETRI, Korea
Dr. Jin Woo HONG, Electronics and Telecommunications Research Inst., Korea
Dr. Heeseok Choi, KISTI(Korea Institute of Science and Technology Information), korea
Dr. Somkiat Kitjongthawonkul, Australian Catholic University, St Patrick's Campus, Australia
Dr. Dae Won Kim, ETRI, Korea
Dr. Ho-Jin CHOI, KAIST(Univ), Korea
Dr. Su-Cheng HAW, Multimedia University, Faculty of Information Technology, Malaysia
Dr. Myoung-Jin Kim, Soongsil University, Korea
Dr. Gyu Myoung Lee, Institut Mines-Telecom, Telecom SudParis, France
Dr. Dongkyun Kim, KISTI(Korea Institute of Science and Technology Information), Korea
Prof. Yoonhee Kim, Sookmyung Women s University, Korea
Prof. Li-Der Chou, National Central University, Taiwan
Prof. Young Woong Ko, Hallym University, Korea
Prof. Dimiter G. Velev, UNWE(University of National and World Economy), Bulgaria
Dr. Tadasuke Minagawa, Meiji University, Japan
Prof. Jun-Kyun Choi, KAIST (Univ.), Korea
Dr. Brownson ObaridoaObele, Hyundai Mobis Multimedia R&D Lab , Korea
Prof. Anisha Lal, VIT university, India
Dr. kyeong kang, University of technology sydney, faculty of engineering and IT , Australia
Prof. Chwen-Yea Lin, Tatung Institute of Commerce and Technology, Taiwan
Dr. Ting Peng, Chang'an University, China
Prof. ChaeSoo Kim, Donga University in Korea, Korea
Prof. kirankumar M. joshi, m.s.uni.of baroda, India
Dr. Chin-Feng Lin, National Taiwan Ocean University, Taiwan
Dr. Chang-shin Chung, TTA(Telecommunications Technology Association), Korea

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume. 5 Issue. 5

Ontology Modification Using Ontological-Semantic Rules

Anastasia Mochalova*, Victor Zacharov**, Vladimir Mochalov*

** Institute of Cosmophysical Research and Radio Wave Propagation FEB RAS , Mirnaia str. 7, 684034 Paratunka, Kamchatka region, Russia*

***Petersburg State University, Universitetskaya emb. 7-9., 199034 St Petersburg, Russia*

stark345@gmail.com, v.zakharov@spbu.ru, sensorlife@mail.ru

***Abstract*—In this work we consider different types of semantic dictionaries and describe the problems of their construction. We also describe the ontological-semantic rules proposed for ontology modification. We provide examples of such rules and describe the process to generate them. The software implementation of ontology modification using ontological-semantic rules is employed as a component of a question answering system integrated with the ontology.**

***Keyword*— ontology modification, semantic analyzer, basic ontological-semantic rules.**

I. INTRODUCTION

With development of information technologies, the challenges of automated processing of natural language text become more and more urgent. One of the problems of automated text processing is the problem of organizing data storage in a structured way, with various additional information about stored elements — such as relations between these elements, names of these relations, hierarchical dependencies between them, qualificative semantic information etc. Ontologies that are used in many problems of automated text processing (for example, in development of question answering systems ([1-3]) and information retrieval systems ([4]), in classification systems ([5]) and estimation of texts resemblance ([6], [7]), in plagiarism detection ([8]) and disambiguation ([9]), in problems of Semantic Matching in Search [10] and information retrieval [11] etc.), are storages of such kind. Also, ontologies are essential components of Semantic Web technology [12] that becomes more and more popular lately.

Ontology creation and modification is a separate problem that does not have a universal solution in our days. One can distinguish two approaches: manual input (which is a very effort-consuming task requiring contribution from highly qualified specialists who know the domain of the ontology well) and automated input. The authors of the work [13] divide automated data input to the ontology into two stages:

1) automatic or automated input using conventional lexicographic information (encyclopaedic, definition and other dictionaries as well as databases);
2) automatic or automated input using analysis of distributional vocabulary characteristics in corpus of texts.

In this work we propose a method for automatic of an object-oriented ontology modification using ontological-semantic rules of the latter type.

In this work, by ontology modification we mean any of the listed below changes of the ontology:

1) Name change of a Class, Object or relation of the ontology;
2) Removal of a Class, Object or relation from the ontology;
3) Addition of a new Class, Object or relation into the ontology;

We propose the following scheme of ontology modification (see Fig. 1):

1) User feeds the analyzed text in natural language into the system's input;
2) The text proceeds into the input of the ontological-semantic analyzer (the detailed work description of such analyzer is provided in work [2]). The result of the analyzer's work is an ontological-semantic graph (a semantic graph, each node of which has a corresponding class or an object of the ontology).
3) The resulting ontological-semantic graph is fed into the input of the module of automated ontology supplement, which, using special ontological-semantic rules, constructs a request for ontology modification (the details of such request construction and of the ontological-semantic rules will be provided further).

In its work, the ontological-semantic analyzer uses data from the ontology (see [2] for details), together with the module of automated ontology supplement (the ontological-semantic rules lying in the base of the module use information from the ontology).

In our work, we developed and implemented in software a

Manuscript received June 10, 2016. The work was implemented with financial support from the Russian Foundation for the Humanities as part of research project No.15-04-12029 — Software development of an electronic resource with an online version of a Russian-language question answering system.

Mochalova A. V., is with the Institute of Cosmophysical Research and Radio Wave Propagation FEB RAS, Russia (corresponding author to provide phone:+7-924-794-21-82; fax: 8-(41531)-33718; e-mail: stark345@gmail.com).

Zakharov V. P, is with the Saint-Petersburg State University, Russia (e-mail: v.zakharov@spbu.ru).

Mochalov V. A., is with the Institute of Cosmophysical Research and Radio Wave Propagation FEB RAS, Russia (e-mail: sensorlife@mail.ru).

prototype of an ontology modification system using ontological-semantic rules. This system is employed as a component in a question answering system integrated with the ontology. The software implementation of the ontology modification system is based on an expert system (the program [14] has been registered) and a semantic analyzer (the program [15] has been registered).

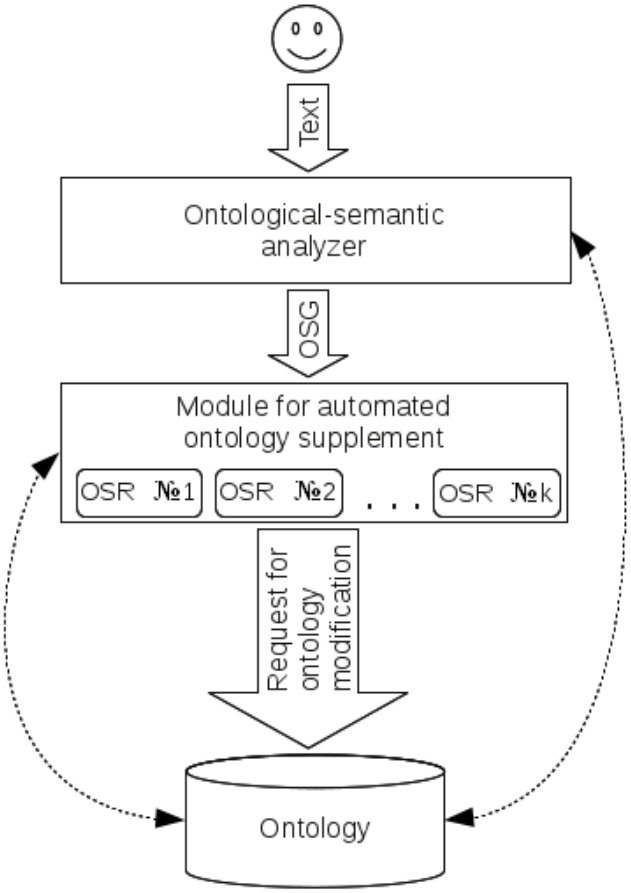


Fig. 1. Workflow of the system implementing automated ontology supplement.

II. Semantic Dictionaries

The work quality of a question answering system strongly depends on completeness and accuracy of the data stored in semantic dictionaries used by the system. These dictionaries are employed in different modules of the QAS, including the syntactic analyzer [16]. In this section we will consider approaches to construct the thesaurus and role models dictionaries; all of them are kinds of semantic dictionaries.

A. A general-purpose thesaurus

A thesaurus in its general sense is a dictionary with semantic relations between dictionary units. Since the end of 1950s, thesauri have been used in systems for machine translation and information retrieval systems (IRS).

In contrast with semantic dictionaries that are intended for detailed description of general lexis, thesauri are created to store and classify the ultimately concrete words and collocations. For example, the word вещество [substance] is in the RGPSD (Russian General-Purpose Semantic Dictionary), while all names of chemical substances are stored in a thesaurus.

Which relationships are described in a thesaurus? As a rule, the following:

1) AKO relationship (see examples in Fig. 2)
2) POF relationship
3) synonymy/antonomy
4) associative relationships.

Relationships stored in ontologies are much more numerous and various.

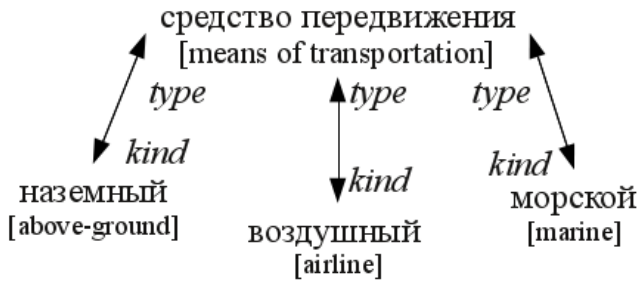


Fig. 2. Example of an AKO relationship

These are paradigmatic relationships (stable relationships between words in a language or in a text). Syntagmatic (textual) relationships are not presented in the thesaurus in an explicit form.

B. Role models dictionaries

Let us employ such approach to semantic text analysis that a sentence is considered as some predicate and a set of arguments. Usually a verb (or another predicate word, e.g., a verbal noun) describing an action acts as a predicate, while actants are the arguments.

When one has constructed a dictionary of verbal role models basing on usage of syntactic and morphological information, it is possible to define roles of nominal groups (arguments) by the predicate, as well as relations between them. For example, one can employ information about a preposition used with the nominal group and the case of the main word of the group. Nevertheless, syntactic information is not always sufficient. Consider an example: "Мы прибыли на автобусе на конференцию на пять дней" [We arrived by bus to a conference for five days]. An example of semantic parsing of this sentence is presented in Figure 3.

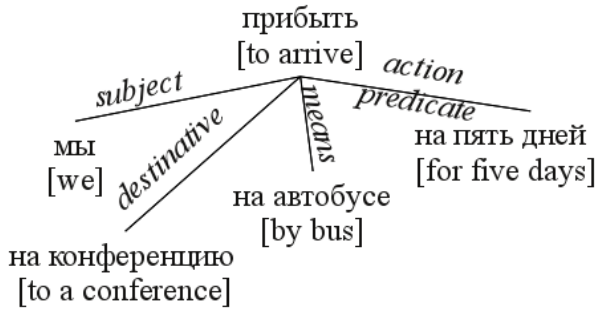


Fig.3. Example of semantic analysis.

The formal attributes (preposition+case) of some nominal groups coincide, so for correct interpretation of such sentence, one additionally needs a thesaurus. In such way, we obtain the following possible appearance of a dictionary entry presented in Table 1. (We assume the occurrence of a thesaurus containing categories "means of transportation" and "time interval").

III. Semantic Relations

In this work we use the term semantic relation (defined below) as the relation defining a link of type "Class-Class", "Class-Object", "Object-Class" or "Object-Object" in the considered object-oriented ontology.

TABLE I
An Example of a Dictionary Entry for the Verb "Arrive".

Role of the verb	Preposition + case of the nominal group	Class of the nominal group
Mean	На [by] + Prepositional case	Means of transportation
Duration	На [for] + Accusative case	Time interval
Object localization	На [to] + Accusative case	Event

By semantic relation we mean a certain universal relation that a native speaker beholds in the language. This connection is binary: it connects two semantic nodes (each of which is a Class or an Object of the ontology) with each other [17]. By semantic nodes we mean syntaxems (syntaxem is an irreducible semantic-syntactic unit conveying primitive categorical meaning and acting as a structural component of a more complicated syntactic composition [18]). Let us say, that two different semantic nodes α and β are connected by the semantic relations R (R(α, β)) if there is a universal binary connection between α and β [17]. Direction of the connection is defined so that the formula R(α, β) would be equivalent to one of the following statements:

1) "β is R for α";
2) "question R can be asked from α to β".

Below you can find examples of the semantic relations equivalent to the first statement:

1) Description(вечер [evening], теплый [warm]);
2) Action(дети [children], пошли купаться [went for a swim);
3) Characteristic_of_action(разоделись [dressed], в пух и прах [to kill]);
4) Time(опоздать [be late], на час [for an hour]).

Below you can find examples of the semantic relations equivalent to the second statement:

1) With_who(прийти [come], с другом [with a friend]);
2) What_for(уронил [drop], нарочно [on purpose]);
3) Whose(мамин [mother's], шарф [scarf]).

It is obvious that these two types of relations are interdependent.

IV. Ontological-Semantic Rules

By an ontological-semantic rule (OSR) we mean the rule of the form «if A, then B» according to which the expert system performs actions described in the right side of the rule in case the conditions described in the left side are held.

Let us put a fact of the expert system into correspondence with each syntaxeme allocated in the analyzed text. By the fact f_i of the expert system we mean a set of six elements: (1) the class or the object of the ontology the syntaxeme belongs to; (2) morphological characteristics of the syntaxeme; (3) ontological characteristics of the syntaxeme; (4) syntaxeme position in the analyzed text; (5) link to the previous fact of the expert system (prev); (6) link to the next fact of the expert system (next). The syntaxeme with the minimal position in the analyzed text (f_0) corresponds to the fact that has link to NULL as the link to the previous fact. The fact with the maximal position in the analyzed text (f_n) has link to NULL as the link to the next fact.

In such way, the analyzed text may be presented as a doubly linked list of facts $F=\{ f_0, f_1, f_2, \ldots, f_n\}$ (see Fig. 4).

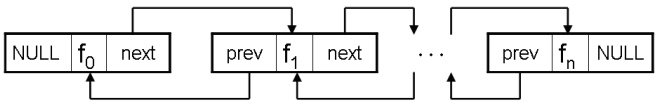


Fig. 4. Doubly linked list of facts of the expert system.

The left side of the rule can contain a doubly linked list of facts and/or Boolean functions having these facts as their arguments.

The right side of the rule contains the list of the actions each of which can modify the ontology of elements corresponding to syntaxemes allocated in the analyzed text. A particular case of the actions performed in the right side of the rule are the functions for ontology modification. The full description of these functions as well as the functions used in the left side of the expert system rules is provided in work [2].

V. Ontology Modification Using Ontological-Semantic Rules

In the Explanatory Dictionary of the Russian Language by Ozhegov [19], the verb is defined as "the part of speech defining an action or a state, expressing this definition in forms of tense, person, number (in the present tense), gender (in the past tense) and forming participles and adverbial participles". The examples from this section of ontology modification are taken from work [20]. We suggest to create OSRs with left sides containing the facts corresponding to the syntaxemes which are verbs. In Fig. 5 we show some functions for work with the ontology (the arrow drawn from the ontology to a function means that the function extracts information from the ontology; the arrow drawn in the opposite direction means that the function modifies data stored in the ontology).

Below we consider an example of modification of an ontology part formed using the following functions (in square brackets we provide functions explanation):

1) CreateClass(172, "страна [country]"); [Create a class "country" with id = 172]
2) CreateClass(1023, "город [city]"); [Create a class "city" with id = 1023]
3) CreateObject(462, 172, "Россия [Russia]"); [Create an object "Russia" with id = 462 belonging to the class with id = 172 (i. e. the class "country")]
4) CreateObject(4017, 1023, "Санкт-Петербург [Saint Petersburg]"); [Create an object " Saint Petersburg" with id = 4017, belonging to the class with id = 10234 (i. e. the class "city")]
5) CreateRelation(7, "Принадлежит [belongs]"); [Create a relation "Belongs" with id = 7]
6) CreateRelation(1023, 172, 7); [Create a relation with id = 7 (i. e. the relation "Belongs" linking the class with id = 1023 (i. e. the class "city") and the class with id = 172 (i. e. the class "country"))]
7) CreateRelation(4017, 462, 7); [Create a relation with id = 7 (i. e. the relation "Belongs" linking the object with id =

4017 (i. e. the object “Saint Petersburg”) and the object with id = 462 (i. e. the object “Russia”))]

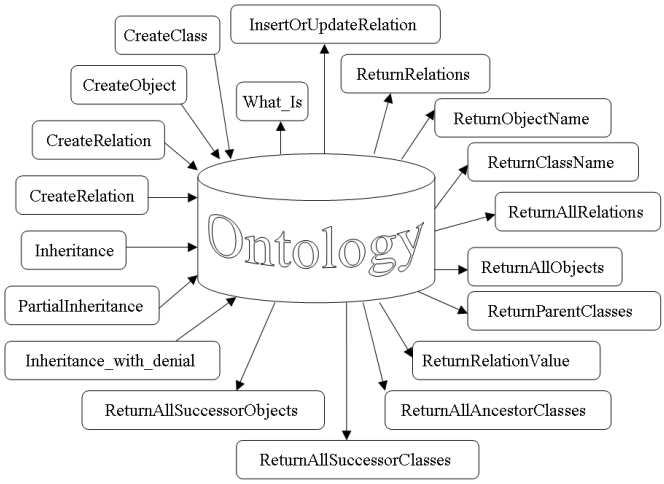


Fig. 5. Functions for work with the ontology.

In Fig. 6 we present the ontology part using the above-described functions. Let us consider the modification process for the ontology a part of which is presented in Fig. 6.

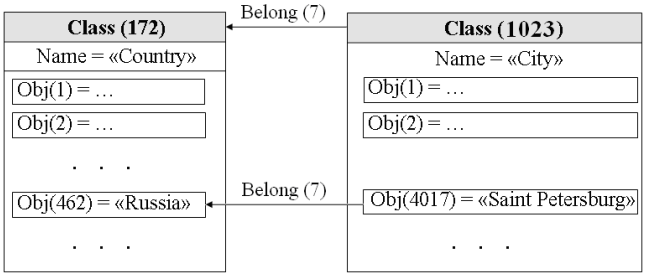


Fig. 6. An example of an ontology part.

Ontological-semantic rules will be applied to the analyzed text presented in one sentence “В августе 1914 года Николай II переименовал Санкт-Петербурга в Петроград [In August 1914, Nikolay II renamed Saint Petersburg into Petrograd]”. With use of the ontological-semantic analyzer described in work [21], we construct an ontological-semantic graph of this sentence (see Fig. 7). Each node of the ontological-semantic graph is a syntaxeme of the analyzed text, written in the lemmatized form. In curly brackets we provide the key ontological information about the corresponding graph node.

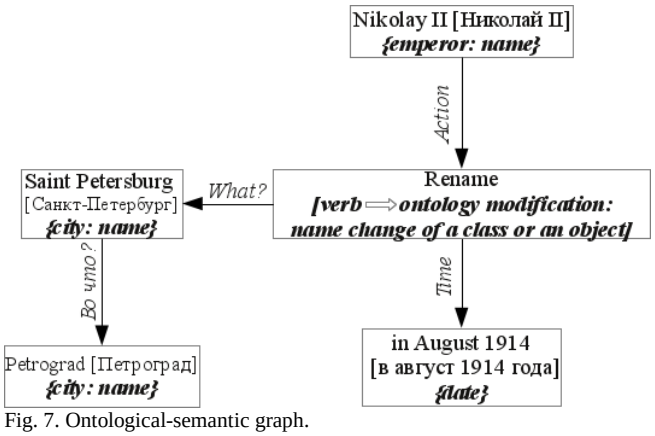


Fig. 7. Ontological-semantic graph.

As a result of the expert system operation using OSRs, modification of the above-decribed ontology will take place: upon expert system performing the OSR containing in its left part the verb “rename”, the name of the object formed previously by the function CreateObject(4017, 1023, "Санкт-Петербург [Saint Petersburg]") will be replaced with “Petrograd”. The information about exact modifications performed, together with their date, will be stored in a log file.

Let us consider another example of the work of the expert system which takes the sentence “В 1878 году по Сан-Стефанскому мирному договору город Батум перешел от Османской Империи к России [In 1878, by the Treaty of San Stefano, the Batum city was seded from Ottoman Empire to Russia]” as its input. Using the ontological-semantic analyzer, we will construct the corresponding ontological-semantic graph on this sentence and modify the existing ontology using the following functions:

1) RemoveRelation(552, 7645, 7); [Remove the relation with id = 7 (i. e. the relation “Belongs”, linking the object with id = 552 (i. e. the object “Batum”) and the object with id = 7645 (i. e. the object “Ottoman Empire”))]
2) CreateRelation(552, 462, 7); [Create a relation with id = 7 (i. e. the relation “Belongs”, linking the object with id = 552 (i. e. object “Batum”) and the object with id = 462 (i. e. the object “Russia”))]

Prepositions play a special role when constructing ontological-semantic rules for ontology modification. A significant part of semantic relations of verbs with other parts of speech is formed using prepositions. Though prepositions have abstract meaning, they manage to organize meaningful context when connecting meaningful parts of speech.

Prepositional constructions used to be described from the grammatical point of view and their semantics used to be neglected. One can hardly mention any corpus-based works dedicated to the Russian prepositions except for the paper by Klyshinsky [22], and a couple of others. It is also difficult to transform a set of constructions into a construction-based dictionary or grammar. To solve this task, one should pay attention to synonymy and variability of the constructions, variability of their grammatical features, and so on. For example, different constructions with the verb прятаться [to hide] differ in dynamical-statical aspect (in Russian meanings of such constructions would depend on the preposition chosen and on the case of the dependent component), while different constructions with the verb ударять [to strike] differ in manner of action (you can strike someone or you can strike the bell: in Russian, these constructions would include different prepositions). Treating constructions this way, we can grasp and describe normal “behavior” of constructions as well as abnormal cases (like the classical Goldberg's example to sneeze the napkin off the table [23]).

Below we provide an example showing how, depending on the context in two different sentences, two different semantic dependencies could be discovered (which means the ontology modification should also differ in the first and in the second case) with equal arguments:

1) Из-за огромных сугробов, наметенных в последнюю метель, экспедиция вышла на неделю позже. [Due to the huge snowbanks drifted by the recent blizzard, the expedition started a week later.] → REASON(выходить [start], из-за сугроб [due to snowbank]))
2) Из-за сугробов вышла маленькая девочка в сером

пальтишке. [A little girl in a gray coat appeared from behind the snowbanks] PLACE(выходить [appear], из-за сугроб [from behind snowbank])

VI. Conclusion

In this work we developed and implemented in software a prototype of a system for ontology modification using a database of ontological-semantic rules. This system is employed as a component of a question answering system using data from the ontology. The ontological-semantic rules for ontology modification were constructed, primarily, considering peculiarities of verbs and prepositions of the Russian language. In their description the rules use both morphological and ontological information about described objects. In the future we plan to extend the base of ontological-semantic rules, and employ context information as well as morphological and ontological information about syntaxemes.

References

[1] R. Sun, J. Jiang, Y. Fan, T. Hang, C. Tat-seng, C. M. Yen Kan, "Using syntactic and semantic relation analysis in question answering", *In Proceedings of TREC*, 2005.

[2] V.A. Kuznetsov, V.A. Mochalov, A.V. Mochalova, "Ontological-semantic text analysis and the question answering system using data from ontology", *ICACT Transactions on Advanced Communications Technology (TACT)*, vol. 4, Issue 4, pp.651-658, July 2015.

[3] A. Mochalova, "Search for answers in ontological-semantic graph", *Proceedings of the AINL-ISMW FRUCT*, Saint-Petersburg, Russia, ITMO University, FRUCT, pp. 174-180, 9-14 November 2015.

[4] M.-H. Hsu, M.-F. Tsai, H.-H. Chen, "Query expansion with conceptnet and wordnet: An intrinsic comparison", *Information Retrieval Technology*, pp. 1–13, 2006.

[5] A. Panchenko, R. Beaufort, H. Naets, C. Fairon, "Towards Detection of Child Sexual Abuse Media: Classification of the Associated Filenames", *In Proceedings of the 35th European Conference on Information Retrieval (ECIR 2013), Lecture Notes in Computer Science*, vol.7814, Moscow, Russia, 2013.

[6] R. Mihalcea, C. Corley, C. Strapparava, "Corpus-based and knowledge-based measures of text semantic similarity", *In AAAI'06*, pp. 775–780, 2006.

[7] G. Tsatsaronis, I. Varlamis, M. Vazirgiannis, "Text relatedness based on a word thesaurus", *Journal of Artificial Intelligence Research*, vol. 37, pp.1–39, 2010.

[8] M. Mozgovoy, V. Tusov, V. Klyuev, "Using measures of semantic relatedness for word sense disambiguation", *Computational Linguistics and Intelligent Text Processing*, vol. 2588 of LNCS, pp. 241–257, Springer Berlin, 2003.

[9] S. Patwardhan, S. Banerjee, T. Pedersen, "Using measures of semantic relatedness for word sense disambiguation", *Computational Linguistics and Intelligent Text Processing*, vol. 2588 of LNCS, pp. 241–257, Springer Berlin, 2003.

[10] H. Li, J. Xu, "Semantic Matching in Search", *Foundations and Trends in Information Retrieval*, vol. 7: No. 5, pp 343-469, 2014.

[11] M. Gupta, M. Bendersky, "Information Retrieval with Verbose Queries", *Foundations and Trends in Information Retrieval*, vol. 9, No. 3-4, pp. 209 – 354, 2015.

[12] G. Antoniu, P. Groth, F. Harmelen, R. Hoekstra, *A Semantic Web Primer*, The MIT Press, Cambridge, Massachusetts, London, England, 288 p., 2012.

[13] V.Sh. Roubashkin, V.A. Kapustin, "Usage of term definitions in encyclopaedic dictionaries for automated ontologies supplement", *XI All-Russian united conference "Internet and the modern society"*, Saint Petersburg, 2008.

[14] A.V. Mochalova, *Certificate of registration of a computer program 'Expert system for search of semantic relations in a Russian-language text using basic semantic rules with removal'*, No. 2016612038, Russia, 17.02.2016

[15] A.V. Mochalova, *Certificate of registration of a computer program 'Program for semantic text analysis basing on basic semantic patterns with removal'*, No. 2015613430, Russia, 28.01.2015.

[16] V.P. Zakharov, A.V. Mochalova, V.A. Mochalov, *Question answering systems. Some problems of automated text processing*, Petrozavodsk: PIN, 40 p., 2015.

[17] A.V. Sokirko, *Semantic Dictionaries and Natural Language Processing*, PhD thesis, Moscow, Russia, 2001.

[18] G.A. Zolotova, *Syntactic Dictionary. The repertoire of the elementary units of Russian syntax*, Moscow, Russia: Nauka, 1988.

[19] S. Ozhegov, N. Shvedova, *Definition dictionary of the Russian language: 80 000 words and phraseological collocations*, Russian Academy of Sciences. Institute of the Russian language named after V.V. Vinogradov. 4th edition, enlarged, Moscow, Azbukovnik, 944 p., 1999.

[20] V.A. Mochalov, A.V. Mochalova, "Ontology modification using basic ontological-semantic rules containing verbs", *Theory and practice of modern humanitarian and natural sciences. Issue 6: collection of research papers of the annual transregional research and application conference*, Petropavlovsk-Kamchatsky, 08-12 February 2016, pp.192-195, 2016.

[21] A.V. Mochalova, "Algorithm for semantic text analysis based on basic semantic patterns with removel", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, No. 5. pp. 126-132, 2014.

[22] E.S. Klyshinsky, N.A. Kochetkova, M.I. Litvinov, Maximov V.Yu., "Automatic construction of collocation database on the base of the big corpus. Computational Linguistics and Intellectual Technologies", *Proceedings of the International Conference "Dialog 2010"*, vol. 9 (16), Moscow, pp. 181–185, June 2010.

[23] A.E. Goldberg, *Constructions at Work: the Nature of Generalization in Language*, Oxford, England: Oxford University Press, 2006.

Anastasia Mochalova was born in Petrozavodsk, Russia, in 1987. She received the bachelor's degree at Petrozavodsk State University, the master's degree in St. Petersburg State University of Aerospace Instrumentation. She is an external PhD student in technical sciences at Petrozavodsk State University. Her research interests include automated processing of natural language texts, development of question-answering systems, automation of ontologies creation, and development of the semantic analyzer.

Victor Zakharov – born Leningradskaya region, USSR, 17.07.1947. Graduated from Leningrad State University (Specialist in Structural and Applied Lingustics, 1970). PhD (Saint-Petersburg State University, Applied and Mathematical Liguistics, 1997). Major field of scientific research is Corpus Linguistics.

He is an Associate Professor, Saint-Petersburg State University. Previous positions ncluded Deputy Director of the Leningrad Center for Scientific and Technical Information, Automation Department Chief in th Russian Academy of Sciences Library. The main publications are as follows: "Corpora of the Russian Language", Text, Speech and Dialogue: Proceedings of the 16th International Conference (TSD 2013, Plzen, Czech Republic), Springer-Verlag (Lecture Notes in Artificial Intelligence, 8082), Berlin-Heidelberg, pp. 1-13, 2013. "Set phrases: a view through corpora", Computational Linguistics and Intellectual Technologies: Proceedings of the International Conference "Dialog 2009" , vol. 14 (21). Moscow, pp. 667-682, June 2015. Current and previous research interests include information retrieval, natural language processing, and computational lexicography.

Dr. Zakharov is a member of the Russian Society of Information Specialists and a member of the Special Interest Group on Slavic Natural Language Processing.

Vladimir Mochalov was born in Lyubertsy, Russia in 1985. He received the Ph.D. degree in electronic engineering from Moscow Technical University of Communications and Informatics. His research interests include networks structure synthesis, artificial intelligence, bio-inspired algorithms, query answering systems, and Big Data.

A performance analysis of optimized semi-blind channel estimation method in OFDM systems

Sangirov Gulomjon*, Fu Yongqing*, Jamshid Sangirov**, Fang Ye* and Ahmad Olmasov***

*Information and Communication Engineering College, Harbin Engineering University, Harbin, 150001 China

**Samsung Electronics, South Korea

***Samarkand branch of Tashkent University of Information Technologies, Uzbekistan

gulomjons@hrbeu.edu.cn

***Abstract* — Nowadays, one of the effectively used technique in wireless communication area is an orthogonal frequency division multiplexing (OFDM). In OFDM systems, channel impairments due to multipath dispersive wireless channels can cause deep fades in wireless channels. Therefore, an accurate and computationally efficient channel state information necessary when coherent detection is involved in the OFDM receiver. Hence, it is essential to have a good channel estimation method for OFDM systems in wireless communication. And normally one of the good channel estimation methods is a semi-blind channel estimation. On the other hand, the semi-blind method requires a large number of processing operations. In order to avoid the high complexity of the existing method, the semi-blind channel estimation has been optimized. At the receiver side, we calculate subspace decomposition for blind channel estimation and further to improve channel estimation we use training based technique to estimate channel state information. Next, we combine these channel estimations as semi-blind channel estimation methods and we optimized semi-blind channel estimation by choosing an optimal technique for training based channel estimation.**

***Keyword*—Semi-blind channel estimation, OFDM, least square and scaled LS**

I. INTRODUCTION

In wideband digital communications the orthogonal frequency division multiplexing (OFDM) is used for splitting a high-rate datastream into number of lower rate streams that are transmitted simultaneously over a number of subcarriers for easy transmission. The OFDM technique is applicable in digital terrestrial multimedia broadcast (DTMB) [1], digital subscriber line (DSL) broadband internet access, wireless network, long term evolution (LTE) [2-3], and 4G the transmitter modulates the message bit sequences into phase shift keying (PSK) / quadrature amplitude modulation (QAM) symbol. And then it performs inverse discrete fourier transform (IDFT) on the symbols for conversion them from the frequency domain to time-domain signals. Usually, next step is the insertion of cyclic prefix (CP) in OFDM system. The reason for the CP is to avoid intercarrier interference (ICI) which occurs by a multipath channel. And it also provides good bandwidth efficiency on the receiver side. In our OFDM system, we use zero padding (ZP) instead of CP. Generally, the ZP replaces nonzero CP by zeros. The ZP-OFDM system has the same spectral efficiency as CP-OFDM system by the condition of the number of zero symbols equals the CP length. Lastly, the transmitter sends the time-domain signals out through a wireless channel.

In OFDM system, a wireless channel plays a big role for the transmission performance. That is why estimating the channel has a significant impact on the efficiency of the transmission performance. We observe one of efficient channel estimation methods that are widely utilized in OFDM systems is called a semi-blind channel estimation. The importance of using a semi-blind channel estimation method is a tradeoff between computational complexity and spectral efficiency. To accomplish channel estimation numerous works subspace decomposition methods have been proposed [4-6]. However, these methods use complex computational schemes that may also reduce spectral efficiency. To improve the spectral efficiency of the channel a subspace pursuit algorithm has been proposed estimation in [7]. This algorithm uses a combination of two algorithms to work for low pilot density, which makes the implementation complicated. A method improving the channel estimation with lower computational difficulty has been introduced in [8]. Nevertheless, it works well when there are few OFDM symbols. Consequently, for working out all symbols the computation amount will be increased. Another method proposed to decrease channel estimation error by subspace estimation bases on a block matrix [9]. But, the calculation and formation of a burst of stacked OFDM symbols create

Manuscript received on February 19, 2016. This work is a follow-up of the invited journal to the accepted out-standing conference paper of the 17th International Conference on Advanced Communication Technology (ICACT2015).

Gulomjon Sangirov is with Modern Communication and Information Systems Research group in the school of Information and Communication Engineering, Harbin Engineering University, Harbin, 150001, China (Corresponding author phone: +86-451-82568266; fax: +86-451-82530010 e-mail: gulomjons@hrbeu.edu.cn).

Yongqing Fu is with Modern Communication and Information Systems Research group in the school of Information and Communication Engineering, Harbin Engineering University, Harbin, 150001, China (e-mail: yongqingfu @hrbeu.edu.cn).

Jamshid Sangirov is with Samsung Electronics, South Korea (e-mail: jamshid@kaist.ac.kr).

Fang Ye is with Modern Communication and Information Systems Research group in the school of Information and Communication Engineering, Harbin Engineering University, Harbin, 150001, China (e-mail: fangye@hrbeu.edu.cn).

Ahmad Olmasov is with telecommunication engineering research group at Samarkand branch of Tashkent University of Information Technologies.

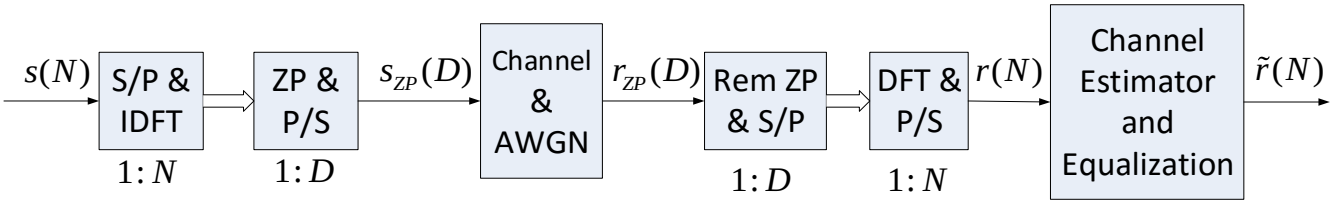


Fig. 1 SISO ZP-OFDM system model

extra complexity by increasing the computational power in channel estimation. A redundant linear precoding based semi-blind channel estimation is developed in [10]. Moreover, it is complex to construct a matrix for semi-blind channel estimation. Therefore, we improved the spectral efficiency and reduced computation complexity of semi-blind channel estimation in single input single output (SISO) OFDM systems. With the intention to evaluate the efficiency of the modified semi-blind channel estimation technique, we compared the simulation results with conventional channel estimation techniques.

II. Description for System Model

In this part, we overview OFDM system model. We consider the system model with a total number of *N* size of OFDM subcarriers. Hence, the m^{th} transmitted block of OFDM symbols can be stated as $\tilde{\mathbf{S}}_N(m) = \left[\tilde{S}_1(m), \cdots, \tilde{S}_N(m)\right]^T$, and here $[\cdot]^{\text{T}}$ is the transpose operator. First, we apply IDFT process and the signal will be

$$\mathbf{s}_N(m) = [s_1(m), \cdots, s_N(m)]^T = \mathbf{F}_N^H \tilde{\mathbf{S}}_N(m) \quad (1)$$

here $\mathbf{F}_N = (1/\sqrt{N}) e^{j2\pi kn/N}$ is IDFT matrix with size N, where $(k = 0, \pm 1, \pm 2..,)$ are discrete Fourier series coefficients. Then we add ZP to $\mathbf{s}_N(m)$, and after that the OFDM symbol becomes $\mathbf{s}_{ZP}(m) = [s_1^{ZP}(m), \cdots, s_D^{ZP}(m)]^T$, here is $D = N + P$, and *P* is the ZP length.

The FIR filter models channel impulse response as $\mathbf{h}_D = [h_0, \cdots, h_{D-1}]^T$. Normally, the channel order size is longer than ZP size which is

$$h_D = \begin{cases} h_i & 0 \le i \le L \\ 0 & else \end{cases}. \quad (2)$$

Hence according to (2) channel parameter vector is assumed as $\mathbf{h} = [h_0, \cdots, h_L]^T$. And in consequence of each transmitting OFDM symbol size, the channel vector could be expressed as following $\mathbf{h}_D = [h_0, \cdots, h_L, 0, \cdots, 0]^T$.

After transmitting $\mathbf{s}_{ZP}(m)$ through the SISO channels, the discrete-time signal from the receiver antenna is given by

$$\mathbf{r}(\mathrm{t}) = \sum_{l=0}^{L} \mathbf{h}(l)\mathbf{s}(t) + \mathbf{n}(t) \quad (3)$$

where $\mathbf{h}(l) = \left[h_1(l), \cdots, h_D(l)\right]$ and $\mathbf{n}(t)$ is additive gaussian white noise (AWGN) with zero-mean and variance σ_n^2.

In the receiver block, the received stacking signal becomes $\mathbf{r}(t), t = mD+1, ..., mD+D$. Hence, the m^{th} intersymbol interference (ISI) free vector can be obtained by the insertion of ZP in the transmitted signal as follows

$$\mathbf{r}_m = \mathbf{H}\mathbf{s}_m + \mathbf{n}_m \quad (4)$$

where **H** is filtering matrix with $D \times D$ lower triangular toeplitz matrix with the first column $[h_0, \cdots, h_L, 0, \cdots, 0]^T$ and the first row $[h_0, 0, \cdots, 0]$. The m^{th} received block of symbols $\mathbf{r}_{ZP}(m)$ can be expressed as

$$\mathbf{r}_{ZP}(m) = \mathbf{H}\mathbf{s}_{ZP}(m) + \mathbf{n}(m). \quad (5)$$

Supposing frequency synchronization and perfect timing, the OFDM demodulator eliminates the ZP and then transform the rest received signals to the frequency domain by DFT for obtaining the frequency domain ZP free received signals. After ZP removal from expression (4), the simplified system mathematical model can be described as

$$\mathbf{R}(m) = \mathbf{H}_N \mathbf{S}_N(m) + \mathbf{N}(m) \quad (6)$$

where $\mathbf{H}_N = \sqrt{N}\mathbf{F}_N \mathbf{h}_N$ is the channel frequency response and $\mathbf{N}(m)$ is AWGN vector after transformation of DFT.

Now let us consider the transmitted m^{th} received block block of OFDM symbols passed through multipath fading channel and m^{th} received signal block became as

$$\mathbf{r}(m) = \mathbf{A}\mathbf{S}_{ZP}(m) + \mathbf{n}(m) \quad (7)$$

where **A = WH**, where **W** is OFDM modulation matrix which consists of $[\mathbf{W}]_{dn} \triangleq W_N^{-(N-1-d)n}$, $n = 0, ..., N-1$, $d = 0, ..., D-1$ and $W_N \triangleq e^{-j2\pi/N}$ and $\mathbf{n}(m)$ is gaussian white noise with variance σ^2. And the problem statement here is the estimation of **H** channel accurately by using fewer pilot signals which contained in received signal.

III. The Channel Estimation

A. Semi-blind channel estimation

First, we estimate the channel in second order statistics blindly because we do not have any information about transmitted signals. The satisfying situation here **H** can be identified blindly up to ambiguity matrix **A**. For subspace channel estimation we calculate singular value decomposition (SVD) of received stacking signal matrix $\mathbf{r}(m)$ according to (7). Or also we can calculate an eigenvalue decomposition (EVD) of autocorrelation matrix of received stacking signal $\mathbf{r}(m)$ which we have

$$\mathbf{R}_{\mathbf{rr}} = \mathbf{H}\mathbf{R}_{\mathbf{ss}}\mathbf{H}^H + \mathbf{R}_{\mathbf{nn}}. \quad (8)$$

And here $\mathbf{R}_{\mathbf{rr}}$, $\mathbf{R}_{\mathbf{ss}}$ and $\mathbf{R}_{\mathbf{nn}}$ notations are the autocorrelation matrix of $\mathbf{r}(m)$, $\mathbf{s}_N(m)$, $\mathbf{n}(m)$ and $\mathbf{R}_{\mathbf{nn}} = \sigma^2 \mathbf{I}_D$, and $\mathbf{I}_D$ is a unit matrix. And the autocorrelation matrices $\mathbf{R}_{\text{rr}}$ and $\mathbf{R}_{\mathbf{ss}}$ stand as full rank. Now we get *D* eigenvalues $\lambda_1, \cdots, \lambda_D$, after performing EVD of $\mathbf{R}_{\mathbf{rr}}$. As the result we have $\lambda_1 \ge \cdots \ge \lambda_N \ge \lambda_{N+1} = \cdots = \lambda_D = \sigma^2$ in descending order, here $\lambda_1, \cdots, \lambda_N$ is an area for the signal subspace, also $\lambda_{N+1}, \cdots, \lambda_D$ is an area for the noise subspace. Suppose we can notate the

noise subspace vector as $\mathbf{g}_i$ ($0 \le i \le L-1$) and due to the orthogonal subspace signal to $\mathbf{g}_i$, we can note that

$$\mathbf{g}_i^H \mathbf{H} = 0 \tag{9}$$

here the channel matrix $\mathbf{H}$ has a similar structure with channel matrix used in (3). Now we can transform (9) equivalently as given

$$\mathbf{G}_i \mathbf{h} = 0 \tag{10}$$

here $\mathbf{g}_i^H$ vector is transformed into $\mathbf{G}_i$ a matrix which consists of $D \times D$ dimension lower triangular toeplitz matrix with the first column $[\mathbf{g}_0^H, \cdots, \mathbf{g}_L^H, 0, \cdots, 0]^T$ and the first row $[\mathbf{g}_0^H, 0, \cdots, 0]$ and $\mathbf{h}$ is same as described in (2).

The calculation of (10) will take more computation, therefore, computation of $\mathbf{G}_i$ can be eliminated by transforming it to

$$\mathbf{Q} = \sum_{i=0}^{L-1} \mathbf{G}_i^H \mathbf{G}_i \ . \tag{11}$$

And further calculating it in the quadratic equation $q(\mathbf{h}) = 0$ which is

$$q(\mathbf{h}) = \mathbf{h}^H \mathbf{Q} \mathbf{h} = \mathbf{0}. \tag{12}$$

In the other hand minimization of $q(\mathbf{h})$ can cause $\mathbf{h}$=0 for that reason, minimization should be focused on the selection of proper constraint. Normally natural constraint would be $\|\mathbf{h}\| = 1$ because in the receiver side the received signal power is roughly constant in practice. Therefore estimating $\mathbf{h}$ channel is unit-norm eigenvector related to the smallest eigenvalue of $\mathbf{Q}$ which is

$$\tilde{\mathbf{h}}^H \mathbf{Q} \tilde{\mathbf{h}} = \mathbf{0}. \tag{13}$$

The calculation of blind methods is slow in convergence rate that is why it is better to use a few pilots for getting the channel knowledge and get initial channel estimation to decrease complication of the channel estimation. Assume we have N_{pil} pilots as frequency domain signal in the transmitter which is $\tilde{S} = \left[\tilde{S}_{pil}(1), \cdots, \tilde{S}_{pil}(N_{pil}) \right]$. At the receiver, received frequency domain pilot signals are $\tilde{R} = \left[\tilde{R}_{pil}(1), \cdots, \tilde{R}_{pil}(N_{pil}) \right]$. Now we can calculate a least square (LS) channel estimation of pilot signal is

$$\tilde{\mathbf{H}}_{LS} = \left[\frac{\tilde{R}_{pil}(1)}{\tilde{S}_{pil}(1)}, \cdots, \frac{\tilde{R}_{pil}(N_{pil})}{\tilde{S}_{pil}(N_{pil})} \right]. \tag{14}$$

Now we can write as $\tilde{\mathbf{H}}_{pil} = \tilde{\mathbf{H}}_{LS}$ and it can be described as the time domain training based channel estimation

$$\tilde{\mathbf{h}}_{pil} = \mathbf{F}_{pil}^H \tilde{\mathbf{H}}_{pil} \tag{15}$$

here $\mathbf{F}_{pil}$ is DFT matrix of the pilot signals. This condition is true when $\mathbf{F}_{pil}$ consists of first *L+1* columns of $\mathbf{F}_N$. And a number of selected rows matches with the pilot signals number.

Let us bring up the system of the equations as

$$\begin{cases} \tilde{\mathbf{h}}^H \mathbf{Q} \tilde{\mathbf{h}} = 0 \\ \mathbf{F}_{pil} \tilde{\mathbf{h}}_{pil} = \tilde{\mathbf{H}}_{pil} \end{cases}. \tag{16}$$

Meanwhile, the system of equations are calculated in the least square sense, therefore quadratic equation can be minimized as

$$q(\mathbf{h}) = \tilde{\mathbf{h}}^H \mathbf{Q} \tilde{\mathbf{h}} + \| \mathbf{h} - \tilde{\mathbf{h}}_{pil} \|^2 \tag{17}$$

here $\mathbf{h}$ is a true channel with the same size pilot signal. And the difference of pilot symbols alone are not enough for the estimation of the channel, therefore, the channel estimation $\hat{\mathbf{h}}$ can be approximated as

$$\hat{\mathbf{h}} = \left(\mathbf{Q} + \mathbf{I}_{\mathbf{Q}} \right)^{-1} \tilde{\mathbf{h}}_{pil} = \boldsymbol{\alpha} \tilde{\mathbf{h}}_{pil} \tag{18}$$

here $\mathbf{I}_{\mathbf{Q}}$ is a unit matrix which is equivalent to $\mathbf{Q}$ the matrix and $\boldsymbol{\alpha}$ is a relational factor between $\mathbf{h}_{pil}$ and $\hat{\mathbf{h}}$, on the other hand, $\boldsymbol{\alpha}$ can also be interpreted as optimization matrix which is actual channel parameter can be approached by $\mathbf{h}_{pil}$.

B. Optimization in semi-blind channel estimation

To obtain the signal and noise subspaces for semi-blind channel estimation we need the actual true $\mathbf{R}_{\mathbf{rr}}$ autocorrelation matrix. In the real practice, the $\mathbf{R}_{\mathbf{rr}}$ is estimated by dividing to M blocks by

$$\tilde{\mathbf{R}}_{\mathbf{rr}} = \frac{1}{M} \sum_{m=0}^{M-1} \mathbf{r}_{ZP}(m) \mathbf{r}_{ZP}(m)^H \tag{19}$$

here M is the number of the received signals. The $\tilde{\mathbf{R}}_{\mathbf{rr}}$ closes to $\mathbf{R}_{\mathbf{rr}}$ unlimitedly when *M* inclines to infinite. And the essential condition for performing EVD decomposition the $\tilde{\mathbf{R}}_{\mathbf{rr}}$ must be full-rank. For this reason, we must ensure that there have to be enough received symbols in the receiver. We can also describe (19) in the following way

$$\tilde{\mathbf{R}}_{\mathbf{rr}} = \mathbf{H} \tilde{\mathbf{R}}_{\mathbf{ss}} \mathbf{H}^H + \mathbf{R}_{nn} \tag{20}$$

which is here

$$\tilde{\mathbf{R}}_{\mathbf{ss}} = \frac{1}{N} \sum_{k=0}^{N-1} \mathbf{s}_M(k) \mathbf{s}_M(k)^H \tag{21}$$

Now we perform EVD of $\tilde{\mathbf{R}}_{\mathbf{rr}}$ and we obtain new $\mathbf{Q}$ matrix, which we rewrite as $\tilde{\mathbf{Q}}$. Subsequently, the initial time domain blind channel estimation is an unit-norm eigenvector related to the smallest eigenvalue of $\tilde{\mathbf{Q}}$ which can also be described by $\tilde{\mathbf{h}}_{\mathbf{Q}}$. Thus we can rewrite (13) as follows

$$\tilde{\mathbf{h}}_{\mathbf{Q}}^H \tilde{\mathbf{Q}} \tilde{\mathbf{h}}_{\mathbf{Q}} = \mathbf{0}. \tag{22}$$

Let us also try to choose optimal computation of LS method by applying the Scaled LS (SLS) channel estimation from [11]

$$\tilde{\mathbf{H}}_{\mathrm{SLS}} = \frac{\mathrm{tr}\left\{ \mathbf{R}_{\mathrm{HH}} \right\}}{\sigma^2 \mathrm{tr}\left\{ \left(\tilde{S} \tilde{S}^{\mathrm{H}} \right)^{-1} \right\} + \mathrm{tr}\left\{ \mathbf{R}_{\mathrm{HH}} \right\}} \tilde{\mathbf{H}}_{\mathrm{LS}} \tag{23}$$

here $\mathbf{R}_{\mathrm{HH}}$ is autocorrelation matrix of $\mathbf{H}$, $\tilde{S}$ is N_{pil} pilots frequency domain signal and $\mathrm{tr}\{\cdot\}$ is a trace of a matrix.

The $\mathrm{tr}\left\{ \mathbf{R}_{\mathrm{HH}} \right\}$ trace is not a limiting factor than knowing of $\mathbf{R}_{\mathrm{HH}}$, which also less limiting than even knowing of $\mathbf{H}$ itself. In simulation, the condition of knowing $\mathrm{tr}\left\{ \mathbf{R}_{\mathrm{HH}} \right\}$ can be replaced by LS estimator which by using the LS-based consistent instead of $\mathbf{H}$ as

$$\mathrm{tr}\left\{ \hat{\mathbf{R}}_{\mathrm{HH}} \right\} = \mathrm{tr}\left\{ \tilde{\mathbf{H}}_{\mathrm{LS}}^{\mathrm{H}} \tilde{\mathbf{H}}_{\mathrm{LS}} \right\}. \tag{24}$$

Now we can use (24) instead of $\mathrm{tr}\left\{ \mathbf{R}_{\mathrm{HH}} \right\}$ in (23). A resulting training based channel estimator become as the LS-SLS estimator $\tilde{\mathbf{H}}_{LS-SLS}$ and we can change to $\tilde{\mathbf{H}}_{pil} = \tilde{\mathbf{H}}_{LS-SLS}$.

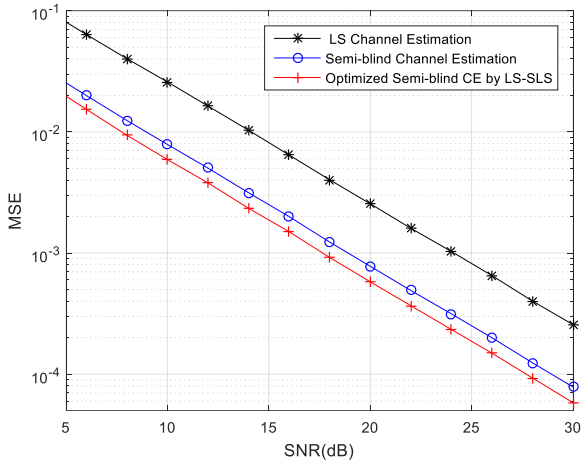


Fig.2 MSE results by using QPSK modulation in OFDM system.

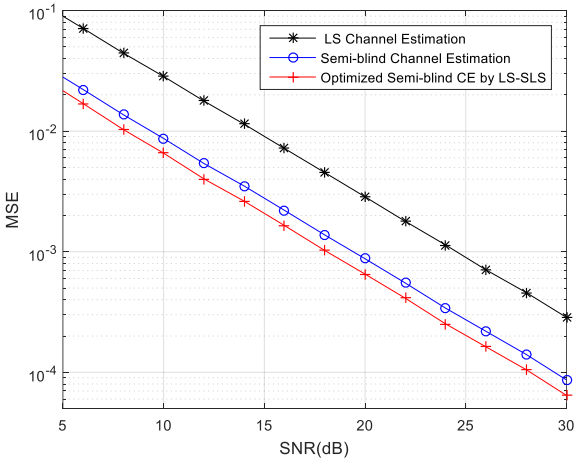


Fig.4 MSE results by using16 QAM modulation in OFDM system.

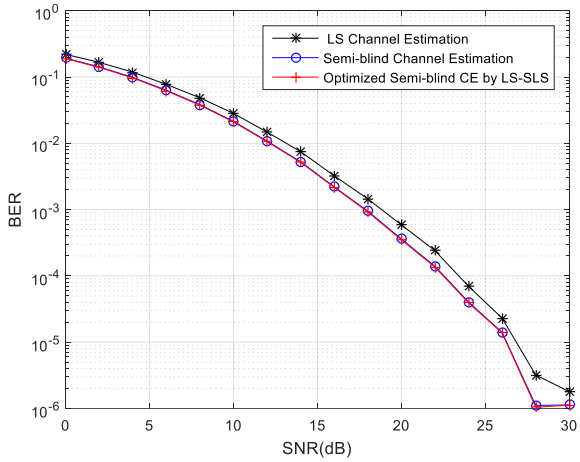


Fig.3 BER vs. SNR results on the basis of QPSK in OFDM system.

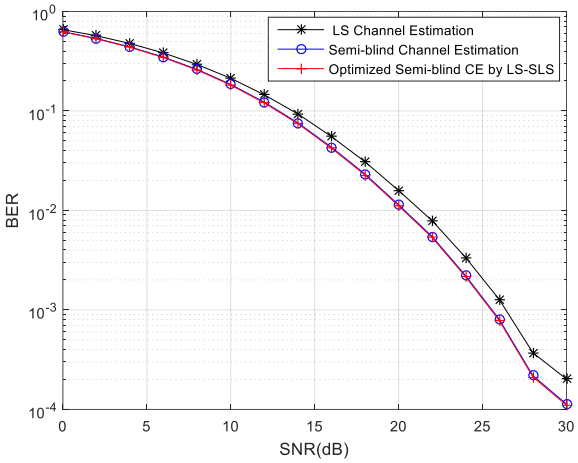


Fig.5 BER vs. SNR results on the basis of 16 QAM in OFDM system.

Correspondingly, the channel information in (18) can be modified as

$$\hat{\mathbf{h}}_{modified} = \left(\tilde{\mathbf{Q}} + \mathbf{I}_{\mathbf{Q}}\right)^{-1} \tilde{\mathbf{h}}_{pil} = \tilde{\boldsymbol{\alpha}}\tilde{\mathbf{h}}_{pil}. \quad (25)$$

But, here it is difficult to satisfy the equation (22) because the noise channel, the $\tilde{\mathbf{Q}}$ matrix contain the noise power.

For this reason, let error of (22) be as follows

$$e = \tilde{\mathbf{h}}_{\mathbf{Q}}{}^{H} \tilde{\mathbf{Q}} \tilde{\mathbf{h}}_{\mathbf{Q}}. \quad (26)$$

Henceforth $e \neq 0$, now the orthogonality condition of initial time domain blind channel estimate and noise subspace is damaged due to the interference of noise. We consider the system estimation error e have been initiated by noise. As a result, one favorable way for improving the system estimation performance is removing the estimation error from $\tilde{\mathbf{Q}}$ matrix as follows

$$\tilde{\mathbf{Q}}_{recomposed} = \tilde{\mathbf{Q}} - e\mathbf{I}_{\mathbf{Q}}. \quad (27)$$

So a new relational factor coefficient defined by $\boldsymbol{\beta}$ such as

$$\boldsymbol{\beta} = \left(\tilde{\mathbf{Q}}_{recomposed} + \mathbf{I}_{\mathbf{Q}}\right)^{-1}. \quad (28)$$

Corresponding to (25), we can achieve optimized semi-blind channel estimation as follows

$$\hat{\mathbf{h}}_{opt} = \boldsymbol{\beta}\hat{\mathbf{h}}_{pil} \quad (29)$$

Targeting to achieve an improved channel estimation performance, we can calculate $\tilde{\boldsymbol{\alpha}}$ as in (18) and dip this relational factor to (29), as given

$$\hat{\mathbf{h}}_{opt} = \boldsymbol{\beta}\tilde{\boldsymbol{\alpha}}\tilde{\mathbf{h}}_{pil}. \quad (30)$$

IV. Simulation Results

In the simulation results for improving the performance of the system, we decreased the noise interference and also modified the channel estimate in proposed semi-blind estimation. During simulation process, we used for each OFDM symbol N=64 subcarriers and the ZP with the length of 16. For the channel, we used the Rayleigh multipath fading channel. In the receiver part, we used zero forcing equalizer in corresponding to the result of channel estimation on the transmission channel. And we denoted the channel estimation as (CE) in the figures. Also for getting results in all simulation runs, we averaged the results by over 4000 Monte-Carlo runs. In Fig. 2 QPSK modulation is used to compare the MSE of our proposed semi-blind channel estimation with LS estimation and conventional semi-blind channel estimation. The proposed semi-blind channel estimation is optimized by the LS-SLS channel estimation. We can see from the simulation results that the optimized semi-blind channel estimation outperformed the conventional semi-blind channel estimation by 1.5-2 dB and LS channel estimation by 6-6.5 dB. In Fig. 3 a bit error rate (BER) verses to signal noise ratio (SNR) is calculated and same methods was compared in Fig. 2. From the result, it is appearing that the proposed semi-blind channel estimation has a similar result with conventional semi-blind channel estimation but still both of them have

better results than LS channel estimation. However, they performed better on 28 dB than 30 dB. Thus we conclude that semi-blind and proposed semi-blind CEs performing better in lower 28-30 dB in our system on the basis of QPSK modulation.

We also applied the QAM 16 modulation in our simulation for showing our proposed channel estimation objectively. And we have calculated MSE comparison in QAM 16 modulation and the simulation result shows that our proposed semi-blind channel estimation still outperform other channel estimation methods. Also, the BER comparison was calculated in Fig. 5 from the result we can see BER performance of the proposed semi-blind channel estimation has also the same result with conventional semi-blind channel estimation but in higher SNR it is still performing better than the result of Fig. 3. However, it has less BER performance in lower SNR, the reason for that is 16 QAM modulation scheme. Because of 16 QAM, modulation scheme consumes more energy than QPSK modulation. For instance to transmit four bits for each 16 QAM symbol rather than the transmitting the two bits per QPSK symbol.

In more demonstrating purpose of our proposed method, we also used normalized estimation mean square errors (NMSE) as expressed in [12]

$$\mathrm{NMSE} = \min_{\mathrm{t}} \frac{1}{N_w} \sum_{w=1}^{N_w} \frac{\left\| \hat{\mathbf{h}}_{\mathbf{w}} \mathbf{t}^{-1} - \mathbf{h} \right\|_F^2}{\left\| \mathbf{h} \right\|_F^2} \qquad (31)$$

where w is a number of iteration, $\|\cdot\|_F$ is the Frobenius norm and $\mathbf{t}$ taken from $\hat{\mathbf{h}} = \mathbf{ht}$ which we called relative coefficient between estimated and actual channel values. Consequently, Fig.6 and Fig. 7 have been calculated in NMSE. And the results show that the proposed method outperforms in NMSE analysis as well. Therefore, we concluded that the proposed method is outperforming in both MSE and NMSE cases.

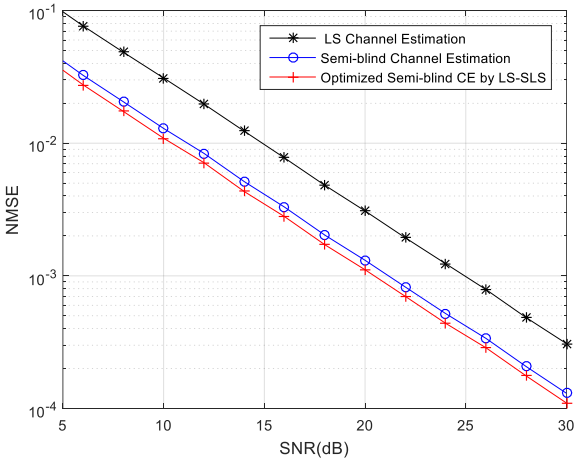


Fig. 6 NMSE of CEs in OFDM system on the basis of QPSK with N_w *=4000*.

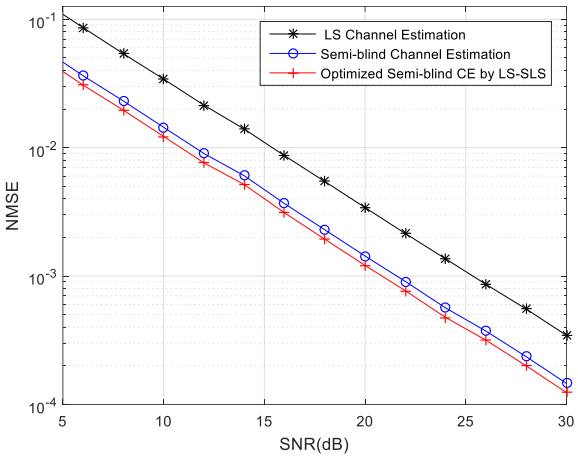


Fig. 7 NMSE of CEs in OFDM system on the basis of 16 QAM with N_w *=4000*.

V. Conclusion

In this research paper, we simulated a number of estimation methods for SISO ZP-OFDM system. The purpose of using ZP features in OFDM is a simplification of the system in the implementation part. The first condition of the channel is that it estimated up to ambiguity matrix by using subspace decomposition. As the simple sequence of the conventional semi-blind channel estimation, the second condition was estimated ambiguity matrix by pilot signals. In the proposed semi-blind channel estimation method, we eliminated subspace decomposition estimation error which is caused by noise in the channel. Further, we have used training based LS-SLS channel estimation for optimization of proposed semi-blind channel estimation. From the simulation results of MSE and NMSE, we can see that the proposed optimized semi-blind channel estimation method outperforms conventional semi-blind channel estimation. And the proposed optimized semi-blind channel estimation method is applicable to various modulations such as phase shift keying (PSK) and quadrature amplitude modulations (QAM).

Acknowledgment

The authors thank the editors, Prof. Yongqing Fu, Prof. Fang Ye, and special thanks to Dr. Jamshid Sangirov.

References

[1] L. Suyue, J. Xiong, L. Gui, and Y. Xu, "A generalized analytical solution to channel estimation with inter-symbol interference cancelation and co-channel interference cancelation for single input single output/multiple input single output digital terrestrial multimedia broadcasting systems", *IEEE Transactions on Broadcasting*, vol. 59, no. 1, pp. 116-128, 2013.

[2] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "LTE-advanced: next-generation wireless broadband technology", *IEEE Wireless Communication*, vol. 17, no. 3, pp. 10-22, 2010.

[3] E. Dahlman, S. Parkvall and J.Sköld, *4G LTE/LTE-Advanced for Mobile Broadband*, *Elsevier* , ISBN: 978-0-12-385489-6, 2011

[4] Buchoux V., Cappe, O., Moulines É., and Gorokhov A., "On the performance of semi-blind subspace-based channel estimation", *IEEE Transactions on Signal Processing*, 48(6), 1750-1759, 2000.

[5] Zeng Y., Lam W. H., and Ng. T. S., "Semiblind channel estimation and equalization for MIMO space-time coded OFDM", *IEEE Transactions on Circuits and Systems I*, vol. 53, no. 2, pp. 463-474, 2006.

[6] Yu J. L., and Lin, Y. C. "Space–Time-Coded MIMO ZP-OFDM Systems: Semiblind Channel Estimation and Equalization", *IEEE Transactions on Circuits and Systems I*, 56(7), pp. 1360-1372, 2009.

[7] Wu W. R., Chiueh R. C., and Tseng, F. S., "Channel estimation for OFDM systems with subspace pursuit algorithm", *IEEE International Conference on Green Circuits and Systems (ICGCS)*, pp. 269-272, 2010.

[8] Fang S. H., Chen J. Y., Shieh M. D., and Lin, J. S. "Modified Subspace Based Channel Estimation Algorithm for OFDM Systems", *IEEE 69th Conference on Vehicular Technology*, pp. 1-5, 2009.

[9] J. Lang Yu, D.-Y. Hong, "Subspace channel estimation assisted block matrix scheme for ZP-OFDM systems", *6th International Conference on Wireless and Mobile Communications (ICWMC)*, pp.16 – 20, 2010.

[10] Huo W., Wang Z., and Li S., “A simple subspace-based semi-blind channel estimator for precoded OFDM systems”, *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, pp. 41-44, 2007.
[11] Biguesh Mehrzad and Alex B. Gershman, "Training-based MIMO channel estimation: a study of estimator tradeoffs and optimal training signals", *IEEE Transactions on Signal Processing* , vol. 54, no. 3, pp. 884-893, 2006.
[12] Gao Feifei and A. Nallanathan, “Subspace-based blind channel estimation for SISO, MISO, and MIMO OFDM systems”, *In IEEE International Conference on. Communications (ICC'06)*, p. 3025-3030, 2006.

Gulomjon Sangirov received the M.S. degrees in Information and Communication Engineering from Harbin Engineering University in 2012. And he is studying Ph.D. in College of Information and Communication Engineering in Harbin Engineering University, China currently. His research interests are Channel Estimation in MIMO-OFDM and Quasi-Cyclic-LDPC coding.

Yongqing Fu received the MS degree in electrical engineering from National University of Defense Technology, Changsha, China in 1985. He held the posts of Lecturer (1988-1995), Associate professor (1995-2000) and Professor (since 2000) in the Electrical Engineering Department, Harbin Engineering University. He was a visiting Professor of Electrical and Computer Engineering Department, University of Manitoba, Canada in 2002 and also Electrical and Computer Engineering Department, University of California, San Diego, the USA in 2009. He is the author of four books, more than 100 articles, and more than 10 patents. His research interests include the weak signal detection, chaotic communication and signal processing, cognitive radio system, image coding, marching and feature extraction and circuit and electronic system. Prof. Fu is the Vice director of the Northeast Electric Theory Association (since 2003), and he is a reviewer for the Journal of China Universities of Posts and Telecommunications (since 2006).

Jamshid Sangirov received the M.S. degrees in Information and Communication Engineering from Yeungnam University in 2006. He got his Ph.D. in Information and Communication Engineering at Korean Advanced Institute of Science and Technology (KAIST) at 2013. He worked with the RFIC Design Team, at Teltron Inc., Korea, from 2010 to 2011. From 2013 he is with Samsung Electronics. His research interests are analog/RF/VLSI and high-speed Integrated Circuit design.

Fang Ye received her Ph.D. degree in Communication and Information System from Harbin Engineering University in 2006. From November 2007 to November 2008, she has been as a visiting scholar in the school of electronics and computer science, University Of Southampton, U.K. Since December 2008, she is an associate professor of the school of Information and Communication Engineering in Harbin Engineering University, China. Her research interests include LTE technologies, adaptive radio resource allocation technology, and UWB signal processing. She is a member of IEEE and Association for Computing Machinery (ACM).

Ahmad Olmasov received the M.S. degrees in Tashkent University of Information Technologies, Tashkent, Uzbekistan in 2007. And he started working with Samarkand branch of Tashkent University of Information Technologies. Currently, he is a lecturer in the department of telecommunication engineering at Samarkand branch of Tashkent University of Information Technologies. His research interests are Mobile communication, channel coding in high throughput wireless communication and MIMO-OFDM.

Terminal-based Energy-Efficient Resource Allocation in OFDMA-Based Wireless Multicast Systems

Jun Liu

Research and Application Innovation Center for Big Data Technology in Railway, Institute of Computing Technologies, China Academy of Railway Science, Beijing, China

junliu04@163.com

***Abstract*—At present, the user experience provided by smart mobile terminals is limited to the battery capacity. This paper focuses on how to improve the energy efficiency of terminals in OFDMA-based wireless multicast systems with frequency-selective channels. We assume that multicast terminals can switch to sleep mode during the transmission of some OFDM symbols according to their OFDMA frame-level quality of service (QoS) requirements. Based on it, we combine resource allocation with terminal sleeping mechanism, and propose a new resource allocation problem model. The task is to minimize the total time when terminals are in receive mode through jointly optimizing the subcarrier allocation for different multicast terminals and the power allocation between different subcarriers, which is a NP-hard problem. To adapt to the needs of real-time applications, we separate subcarrier and power allocation, and propose a low-complexity suboptimal algorithm for this problem. Performance evaluations are conducted in homogenous and heterogeneous networks respectively. Simulation results show that compared with traditional multicast and unicast, our proposed method reduce the total energy consumption of terminals significantly with the same QoS requirements of terminals guaranteed. Additionally, the advantage of our proposed method over traditional multicast diminishes with the increase of the maximum transmission power, and increase with the number of multicast terminals and OFDM symbols in an OFDMA frame.**

***Keyword*—Energy Consumption, Terminal, Resource Allocation, OFDMA, Multicast**

I. INTRODUCTION

With the development of smart mobile devices and communication technology, the mobile traffic is growing significantly in recent years, which stimulates the research of green communication. Since base stations occupy the most of energy consumption, the majority of the related research works were conducted from the perspective of base stations. Actually, the development of mobile applications makes user experience more and more limited to the battery capacity. Therefore, it makes sense to improve the energy efficiency of terminals.

Both multicasting and orthogonal frequency division multiple access (OFDMA) are identified as efficient techniques to address the challenge of limited system resources. In OFDMA-based wireless multicast system, resource allocation is an effective technique that can improve the spectrum efficiency compared to traditional multicast [1], [2], [3]. In [4] and [5], it is proved that clustering the multicast terminals can increase the spectrum efficiency further. It should be pointed out that in the clustering scheme no subcarrier can be shared by multiple clusters, which is referred to as Scheme I. Reference [6] assumed that each subcarrier can be allocated to all the multicast terminals, which is referred to as Scheme II. Scheme I means that a terminal that does not belong to the allocated terminals of a subcarrier may have a better channel condition on this subcarrier. If the allocated terminals can receive the transmitted message on the subcarrier, the terminal with a better channel condition will definitely receive the same message. Accordingly, Scheme II can utilize the transmission resource more efficiently than Scheme I. However, [6] did not take the QoS requirements of terminals into account. And the above research works do not consider the energy efficiency of multicast terminals. References [7] and [8] studied the energy efficiency of multicast terminals through resource allocation based on OFDMA system. Nevertheless, in [7] the channel conditions on all the subcarriers are assumed the same, which ignores the frequency-selective channels. And the energy consumption model of terminals in [8] needs to be improved to adapt to the OFDMA-based system more effectively.

In this paper, we aim at reducing the energy consumption of terminals in OFDMA-based multicast system with the QoS requirements of terminals guaranteed for the frequency-selective channels. In our system, each subcarrier can be allocated to all the multicast terminals. We combine resource allocation with terminal sleep model to reduce the energy consumption of terminals. The terminals are switched to sleep mode when their QoS requirements are satisfied during the transmission of each OFDMA frame. The formulated optimization problem is solved using a

Manuscript received March 5, 2016. This work is a follow-up of the invited journal to the accepted conference paper of the 17th International Conference on Advanced Communication Technology.

Jun Liu is with Research and Application Innovation Center for Big Data Technology in Railway, Institute of Computing Technologies, China Academy of Railway Science, Beijing, 100081 China (corresponding author phone: +86-158- 014-999-63; e-mail: junliu04@163.com).

low-complexity algorithm through optimizing the subcarrier allocation and power allocation separately.

The rest of this paper is organized as follows. Section II firstly presents our system model and then formulates the energy efficiency optimization problem in OFDMA-based multicast system. Section III proposed a low-complexity algorithm for the optimization problem. Simulations are conducted in Section IV followed by the conclusions in Section V.

II. System Model And Problem Formulation

A. System Model

The resource allocation model in OFDMA-based multicast system is illustrated in Figure 1. We consider single-cell multicast systems and frequency-selective channels. Furthermore, each subcarrier can be shared by all the terminals. In this paper, the channel condition of each terminal remains constant in an OFDMA frame with block fading. And we assume that the base station have perfect channel state information (CSI) of different terminals on all the subcarriers. In LTE, the CSI can be reported periodically to the base station through physical uplink control channel (PUCCH) from terminals. It is essential for the link adaptation at the base station, including adjusting the transmission rate with adaptive modulation and coding (AMC) [9]. In this paper, the CSI is used by resource allocation algorithm to minimize the energy consumption of terminals with the total transmission power constraint. Dynamic resource allocation means that the allocated subcarriers of each terminal vary in different OFDMA frames. So each terminal will receive different discontinuous parts of the original message. Therefore, we assume that the source content are encoded with erasure coding (e.g., fountain coding) or multiple description coding [10] beforehand so that terminals can recover the original content once the minimum amount of data is received, regardless of the specific received sequence of data. An OFDMA frame consists of symbols in the time domain and subcarriers in the frequency domain. A symbol and subcarrier combination is the minimal allocable unit, which is called a "tile" [7], [11], [12], and each tile can be coded and modulated individually according to the subcarrier and power allocation results. Let c_k be the number of loaded bits on subcarrier k with $c_k \in \{0,1,\ldots$ where M is the maximum number of loaded bits. Let $R^{\min}$ be the minimum rate required by each terminal. As is in [12], it can be transformed into the minimal number of bits in an OFDMA frame required by each terminal $H^{\min}$, referred to as "QoS requirement" in this paper. In the 3GPP technical specification of [9], Discontinuous transmission (DRX) is supported to enable mobile terminal power saving in LTE system. It means that in order to save power, terminals can almost close the receiving module and turn to sleep mode when they do not need to receive information. Moreover, DRX has been introduced to multimedia broadcast/multicast service [13]. Additionally, we refer to [7] and assume that the energy assumption when terminals receive data depends on the time when they are in receive mode. For the OFDMA frame model as shown in figure 1, once the QoS requirement of a terminal is satisfied, this terminal can switch to sleep mode during the transmission of the remaining OFDM symbols. So the consumed energy of terminals is in direct proportion to the number of OFDM symbols they receive. In this paper, energy efficiency is defined as the inverse of the energy consumption of terminals required to satisfy the QoS requirements of terminals.

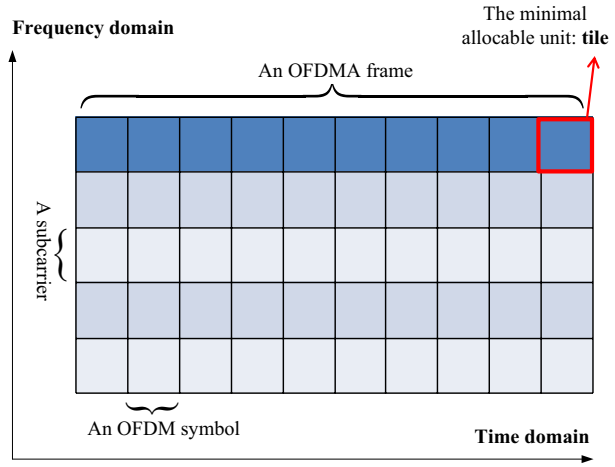


Fig. 1. The resource allocation model in OFDMA-based multicast system

B. Problem Formulation

We consider an OFDMA-based multicast system with K subcarriers and N terminals which request the same data service. There are S symbols in an OFDMA frame. Let $h_{k,n}$ be the channel gain of terminal n on subcarrier k. To ensure that terminal n can decode c_k loaded bit on subcarrier k, the required power p_k should satisfy $p_k \geq f(c_k)/h_{k,n}{}^2$. We consider M-ary quadrature amplitude modulation (M-QAM), then $f(c_k) = \frac{N_0}{3}\left[Q^{-1}(p_e/4)\right]^2\left(2^{c_n}-1\right)$ where p_e is target bit error rate, $N_0/2$ is the variance of additive white Gaussian noise, and $Q^{-1}(x)$ is the inverse function of $Q(x)$ with $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$ [6]. Let $\rho_{k,n}$ be a subcarrier allocation indicator which is 1 if subcarrier k is allocated to terminal n, and 0 otherwise. Note that in our system, the energy consumption of terminals is in direct proportion to the number of OFDMA symbols required to satisfy the QoS requirements of terminals. Accordingly, our problem is formulated as follows

$$\min \sum_{n=1}^{N} \left\lceil \frac{\mathrm{H}^{\min}}{\sum_{k=1}^{K} \rho_{k,n} c_k} \right\rceil \tag{1}$$

$$\text{s.t.} \quad \rho_{k,n} \in \{0,1\}, \forall n, \forall k \tag{2}$$

$$c_k \in \{0,1,...,M\}, \forall k \tag{3}$$

$$\sum_{k=1}^{K} \rho_{k,n} c_k \geq \frac{\mathrm{H}^{\min}}{S}, \ \forall n \tag{4}$$

$$p_k \geq \frac{f(c_k)\rho_{k,n}}{{h_{k,n}}^2}, \forall n, \forall k \tag{5}$$

$$\sum_{k=1}^{K} p_k \leq P_{\max}, p_k \geq 0 \tag{6}$$

where constraint (4) corresponds to the QoS requirements of terminals. $P_{\max}$ represents the maximum transmission power and constraint (6) corresponds to the total transmission power limitation. So our optimization problem is to minimize the total number of OFDMA symbols needed to satisfy the QoS requirements of terminals through optimizing the subcarrier allocation $\{\rho_{k,n}\}$ and the power allocation $\{p_k\}$ /bit allocation $\{c_k\}$. Because p_k is continuous and c_k is discrete, it is much more convenient to search the optimal bit allocation than power allocation. In traditional multicast, the total transmission power is equally allocated to all the subcarriers (i.e., $p_k = P_{\max}/K$, $\forall k$), and each subcarrier is shared by all the terminals (i.e., $\rho_{n,k}=1, \forall n, \forall k$). In this way, the bit rate on each subcarrier is limited by the terminal with the worst channel gain. Thus traditional multicast needs too many OFDM symbols to satisfy the QoS requirements of terminals. In the next section we will investigate how to improve the energy efficiency of traditional multicast.

III. User-based Energy-Efficient Resource Allocation Algorithm

The optimization problem of equation (1)-(6) is a nonlinear integer programming problem. And it is NP-hard [6]. The optimal solution can be derived by exhaustive search. When exhaustive search is used, the number of possible subcarrier allocations is N^k and each possible subcarrier allocation corresponds $(M+1)^K$ possible bit allocations. The optimal combination of subcarrier and bit allocation is the one that makes subjective function the smallest. Therefore, the complexity of exhaustive search is $N^k(M+1)^K$, which makes this method unsuitable for real-time applications. A low-complexity algorithm is necessary for this dynamic resource allocation problem.

The set of the terminals that are allocated subcarrier k can be expressed as $\mathrm{U_k} = \{n : \rho_{n,k} = 1, n \in \{1,2,...,N\}\}$. And the set of the subcarriers that allocated to terminal n can be expressed as $\mathrm{K_n} = \{k : \rho_{n,k} = 1, k \in \{1,2,...,K\}\}$. We define *longitudinal rate* v_n as $v_n = \sum_{k \in K_n} c_k$, which means the total number of loaded bits allocated to terminal n in an OFDMA frame. The energy consumption of each terminal can be expressed as $E_n = \lceil H^{\min}/v_n \rceil$, where $\lceil a \rceil$ means round a to the nearest integer no less than a. Thus when the channel conditions on all the subcarriers are determined, we expect the longitudinal rate of each terminal to be as large as possible to reduce the number of OFDMA symbols required to satisfy the terminals' QoS requirements. Considering the constraint of real-time applications on complexity, we separate subcarrier and power allocation, and propose a low-complexity suboptimal algorithm. In this algorithm, the power allocation remains unchanged during subcarrier allocation, and the subcarrier allocation remains unchanged during power allocation. But bit allocation is changeable in both subcarrier and power allocation.

A. Initial Allocation

Traditional multicast is applied to the initial allocation, i.e., $p_k = P_{\max}/K, \forall k$, and $\rho_{n,k}=1, \forall n, \forall k$. Since the number of loaded bit on subcarrier k is determined by the worst channel condition of $\mathrm{U_k}$ and the power on this subcarrier, it can be calculated according to equation (5) as follows:

$$c_k \leq \left\lfloor f^{-1}\left(p_k \min_{n \in \{1,...,N\}} \left({h_{k,n}}^2\right)\right)\right\rfloor = \left\lfloor \log_2\left(1 + \frac{3p_k \min_{n \in \{1,...,N\}} \left({h_{k,n}}^2\right)}{N_0\left(Q^{-1}(P_e/4)\right)^2}\right)\right\rfloor \tag{7}$$

where $\lfloor a \rfloor$ means round a to the nearest integer no larger than a. Note that $c_k \leq M, \forall k$. In this case, $\mathrm{U_k} = \{1,...,N\}$.

B. Subcarrier Allocation

For simplicity, define *the worst terminal* of subcarrier k as the terminal with the worst channel condition on subcarrier k. Set the maximum number of iteration as $Iter_{\max\_1}$. In each iteration, the following process is conducted for the subcarriers $\{1,...,K\}$ in order. Remove the worst terminal from $\mathrm{U_k}$. On one hand, if terminal n_k^* is removed from subcarrier k, according to equation (7) the number of loaded bit on this subcarrier may increase. This will raise the longitudinal rate of the terminals in $\mathrm{U_k}$ and thus reduce the energy consumption of these terminals. On the other hand, since terminal n_k^* is removed from subcarrier k, the QoS requirement of terminal n_k^* may be no longer satisfied. It requires us to allocate more tiles on other subcarriers for this terminal. In the tile adding process the increased energy consumption (i.e., number of the OFDMA symbols) of terminal n_k^* should be kept as small as possible. Let E_{total} be the current energy consumption of terminals. Let $E_{total}(k)$ be the energy consumption of terminals after removing terminal n_k^* from subcarrier k. Next, update c_k, the longitudinal

rates of each terminals v_n, and $E_{total}(k)$. It is a valid removal if the required number of symbols is less than S after the tile adding process and $E_{total}(k) < E_{total}$. In each iteration, we search subcarrier k^* that minimizes the total energy consumption of terminals. The iteration does not stop until the worst terminal on all the subcarriers cannot be removed or the number of iteration reaches $Iter_{\max\_1}$.

In each iteration, the number of considered allocations is K. Since a terminal may be removed from a subcarrier after each iteration, the maximum number of iterations is KN. Therefore, the maximum number of possible allocations in subcarrier allocation is NK^2. Here the maximum number of iteration is $Iter_{\max\_1}$ which is smaller than KN, so the actual number of possible allocations is $Iter_{\max\_1}K$.

C. Power Allocation

Define the maximum number of iteration as $Iter_{\max\_2}$. During each iteration, we adjust the number of loaded bit on subcarrier k from c_k to c_k+1 and update the required power on this subcarrier as well as the total transmission power $P_{total} = \sum_{k=1}^{K} p_k$. This may violate the transmission power constraint of $P_{total} \le P_{\max}$. So we should choose one of the other subcarrier $\{i : i \in \{1,2,...,K\}, i \ne k\}$ and reduce its power. Specifically, calculate the excess of the transmission power $\Delta P = P_{total} - P_{\max}$ and reduce the power on subcarrier i from p_i to $p_i - \Delta P$. Let $E_{total}(k,i)$ be the total energy consumption of terminals after adjusting c_k and p_i. Then update c_i and $E_{total}(k,i)$. It is a valid adjustment only if $E_{total}(k,i) < E_{total}$. For subcarrier k, we search the subcarrier i^* that achieves the largest decrement of the total energy consumption with the QoS requirements of terminals guaranteed, and reduce its power. Thus $i^* = \arg\min_{i \ne k, i \in \{1,2,...,K\}} (E_{total}(k,i))$. In each iteration, we search the subcarrier pair $\{k^*, j^*\}$ that minimizes the total energy consumption and adjust their power allocation according to the foregoing method. The above process does not stop until the total energy consumption no longer decreases or the number of iteration reaches $Iter_{\max\_2}$.

In power allocation, the maximum number of possible allocations is $(M+1)^K$. Here the maximum number of iteration is $Iter_{\max\_2}$, and the actual number of possible allocations in power allocation is $Iter_{\max\_2}K(K-1)$. Accordingly, the maximum number of possible allocations in the proposed algorithm is $NK^2 + (M+1)^K$, which is usually much smaller than that of exhaustive search, $N^k (M+1)^K$. And the actual number of possible allocations is $Iter_{\max\_1}K + Iter_{\max\_2}K(K-1)$. The pseudocode of the proposed algorithm is summarized in Table I.

TABLE I
THE PSEUDOCODE OF THE PROPOSED ALGORITHM

1) **Initializaiton**:
0. Let $p_k = P_{\max}/K, \forall k$ and $\rho_{n,k}=1, \forall n, \forall k$
1. Calculate c_k according to (7)
2. $K_n = \{k : \rho_{n,k} = 1, k \in \{1,2,...,K\}\}$
3. $v_n = \sum_{k \in K_n} c_k$ and $E_n = \lceil H^{\min}/v_n \rceil$
4. $E_{total} = \sum_{n=1}^{N} E_n$

2) **Subcarrier allocation**:
5. Let iter_i=1
6. For all k do
7. $n_k^* = \min(h_{k,n}^{\ 2})$
8. $U_k = U_k - \{n_k^*\}$, i.e., $\rho_{k,n^*} = 0$
9. Update $E_{n_k^*}$, c_k, and v_n for all n
10. If $E_{n_k^*} > S$ $E_{total}(k) = +\infty$, go to 6; End if
11. $E_{total}(k) = \sum_{n=1}^{N} E_n$
12. End for
13. If $\min_{k \in \{1,2,...,K\}} (E_{total}(k)) > E_{total}$
14. Stop
15. Else if
16. Find $[k^*, n_k^*] = \arg\min_{k \in \{1,2,...,K\}} (E_{total}(k))$
17. $E_{total} = E_{total}(k^*)$ and iter_i= iter_i+1
18. If iter_i= $Iter_{\max\_1}$ stop; else, go to 6.
19. End if

3) **Power allocation**
20. Let iter_i=1
21. For all k do
22. $c_k = c_k + 1$
23. update p_k and P_{total}
24. If $P_{total} \ge P_{\max}$
25. Calculate $\Delta P = P_{total} - P_{\max}$
26. For all $\{i : i \in \{1,2,...,K\}, i \ne k\}$
27. $p_i = p_i - \Delta P$, and update c_i and v_n for all n
28. For all n do
29. If $E_n > S$ $E_{total}(k,i) = +\infty$, go to 26; End if
30. End for
31. Calculate $E_{total}(k,i)$
32. End for
33. End if
34. Find $i^* = \arg\min_{i \in \{1,2,...,K\}, i \ne k} (E_{total}(k,i))$
35. $E_{total}(k) = E_{total}(k,i^*)$
36. End for
37. If $\min_{k \in \{1,2,...,K\}} (E_{total}(k)) > E_{total}$
38. Stop
39. Else if
40. Find $[k^*, j^*] = \arg\min_{k \in \{1,2,...,K\}} (E_{total}(k))$
41. $E_{total} = E_{total}(k^*)$ and iter_i= iter_i+1
42. If iter_i= $Iter_{\max\_2}$ stop; else, go to 21.
43. End if

IV. Performance Evaluation

In the simulations, we use ITU Pedestrian-B channel model [14] to evaluate our proposed method. The path loss model is $L(dB) = 148 + 40\log_{10} d$, where d is in units of meters and stands for the distance to the base station. Rayleigh fading channel is considered. Some system parameters are listed in Table II. The QoS requirements of all the multicast terminals are set to 2500bits/OFDMA frame.

TABLE II
System Parameters

Parameter type	Value
Channel bandwidth	1MHz
Carrier frequency	2000MHz
Number of subcarriers	32
Subcarrier bandwidth	15kHz
Doppler shift	18Hz

Traditional multicast and unicast method are considered for comparison. Furthermore, to have a more thorough evaluation of our proposed method, we considered the combination of traditional multicast and the power allocation of our proposed method, which is denoted as "Traditional multicast+PAO". In unicast each subcarrier can only be allocated to one terminal. Specifically, each subcarrier is only allocated to the terminals with the best channel gain on the subcarrier. To ensure fair comparison, the power allocation of the proposed algorithm is applied in unicast method. In this paper it is called an "outage" event that the QoS requirement of a terminal is not satisfied in an OFDMA frame. The QoS requirements of terminals are satisfied only if the average outage probability of all the terminals is not larger than 5% [15]. In the proposed method, the maximum number of iteration is set to 20.

Beforehand the available number of OFDM symbols in an OFDMA frame is denoted by S . As is analyzed in Section II.A, the energy consumption of terminals can be assumed to be proportion to the number of OFDM symbols they received. So S is the maximal one among all the possible number of OFDM symbols a terminal receives in an OFDMA frame, which corresponds to the maximum energy consumption. For the convenience of comparison, in the following simulations we normalize the simulated energy consumption with respect to the maximum one.

A. Homogeneous Networks

Firstly, we consider homogeneous network where all the multicast terminals experience independent and identically distributed fading with the distance to the base station d =200m. Here we discuss the effects of the maximum transmission power, the number of terminals and the number of OFDM symbols in an OFDMA frame on the total energy consumption of terminals. In the first scenario, the number of terminals N is set to 10 and the available number of OFDM symbols in an OFDMA frame S is set to 60 [7]. The corresponding simulation results are plotted in Fig. 2 where both the proposed multicast and traditional multicast satisfy the QoS requirements of terminals. It can be seen that the proposed multicast achieves much lower energy consumption of terminals. And the average energy consumption decreases as the maximum transmission power increases. Note that in the considered simulation environment, unicast cannot satisfy the QoS requirements of terminals although it consumes the maximum energy. Moreover, it shows that the energy efficiency gain of the proposed method over traditional multicast diminishes with the increase of the maximum transmission power. It can be explained as follows. It is known that the increase of transmission power can improve the average channel condition of terminals. However, the maximum number of loaded bits of each tile M is fixed beforehand, which limits the increase of the terminal rate and thus slowdown the reduction of energy consumption of terminals. Because the proposed method utilizes the relatively better channel gains in a more effective way compared to traditional multicast, it will suffer from the above-mentioned limitation earlier than traditional multicast.

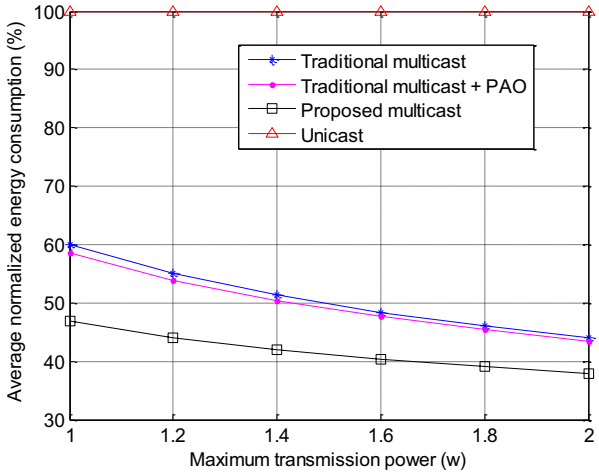


Fig. 2. Energy consumption comparison with different maximum transmission power in homogeneous networks

Specifically, the quantitative relationship between the maximum transmission power and the terminal energy consumption decrement of the proposed method over traditional multicast is listed in Table III. It can be seen that with the maximum transmission power increases gradually in steps of 0.2w starting from 1w, the energy consumption decreasing ratio of the proposed method over the traditional method ranges from 13.829% to 21.898%. And the decreasing ratio diminishes with the increase of the transmission power, which is in accord with Fig. 2.

TABLE III
The Terminal Energy Consumption Decrement of the Proposed Method over Traditional Multicast in Homogeneous Networks

Maximum transmission power (w)	The terminal energy consumption decrement
1	21.898%
1.2	20.184%
1.4	18.377%
1.6	16.640%
1.8	15.109%
2	13.829%

Furthermore, we analyze the marginal terminal energy

consumption decrement with successive and fixed increase of the transmission power for the proposed method. The corresponding results are listed in Table IV. It can be seen that the terminal energy consumption decreases 2.4110%~6.2884% every time the maximum transmission power increases 20% (i. e., increases 20% compared to the initial transmission power of 1w each time) in the considered range. Moreover, with the transmission power increases gradually, the marginal terminal energy consumption decrement of the proposed method phases down. In other words, from the perspective of terminal energy consumption, the marginal effect brought by the maximum transmission power gets smaller with the increase of the maximum transmission power.

TABLE IV
THE MARGINAL TERMINAL ENERGY CONSUMPTION INCREMENT OF THE PROPOSED METHOD IN HOMOGENEOUS NETWORKS

The marginal increment of the maximum transmission power	The marginal terminal energy consumption decrement
0	0
20%	6.2884%
20%	4.4599%
20%	3.3913%
20%	2.6993%
20%	2.4110%

In the second scenario, the maximum transmission power is set to 1.4W with S =60. We evaluate the effects of the number of terminals. The corresponding simulation results are plotted in Fig. 3 where the QoS requirements of terminals are satisfied in both traditional and proposed multicast. In unicast the QoS requirements of terminals are not satisfied when the number of terminals $N \geq 5$. The simulation results show that the advantage of the proposed multicast over traditional multicast increases with the number of terminals. The reason is as follows. For each subcarrier, the more the number of terminals, the higher the probability that the channel condition of a terminal on this subcarrier is bad. As is mentioned before, the transmission rate of traditional multicast is limited to the worst terminal. Therefore, the increase of the number of terminals will prolong the time needed to satisfy the QoS requirements of all the terminals. In comparison, the proposed multicast utilizes both multiuser diversity and frequency-selective fading to allocate the terminals with better channel gains for each subcarrier, which alleviates the constraint of the worst terminal.

In the third scenario, the maximum transmission power is also set to 1.4W and the number of terminals N is set to 10. Here we evaluate the effects of S on the total energy consumption of terminals. The corresponding simulation results are plotted in Fig. 4, where the QoS requirements of terminals are not satisfied only in unicast. The simulation results show that the advantage of the proposed multicast over traditional multicast increases with the number of OFDM symbols S in an OFDMA frame. The reason is that the increase of S means the expansion of optimization zone, which results in better resource allocation.

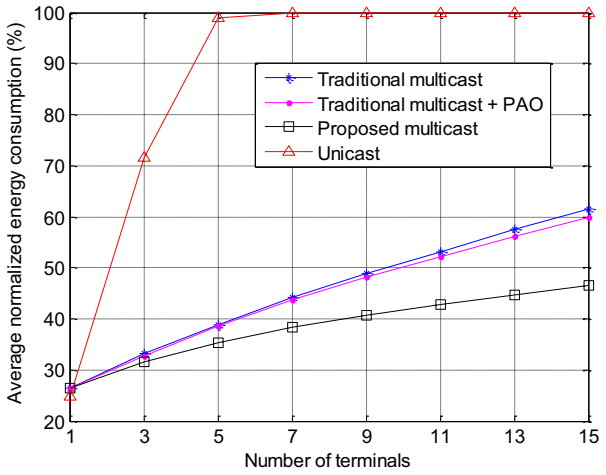


Fig. 3. Energy consumption comparison with different maximum transmission power in homogeneous networks

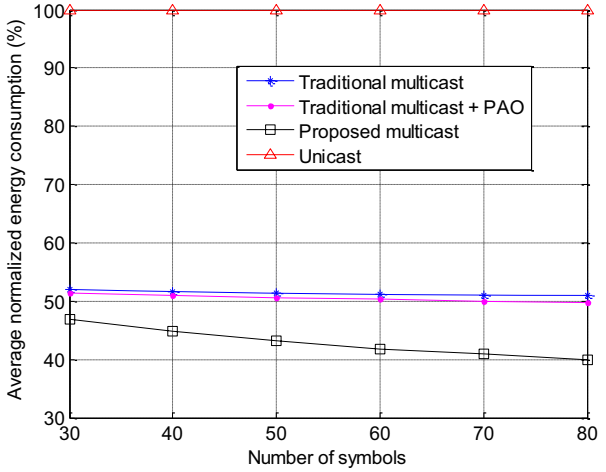


Fig. 4. Energy consumption comparison with different number of OFDM symbols in an OFDMA frame in homogeneous networks

B. Heterogeneous Networks

Then we turn to heterogeneous networks where the multicast terminals experience independent but non-identically distributed fading with the distance to the base station uniformly distributed between 0 and 500m. We also investigate the effects of the maximum transmission power and number of terminals on the energy consumption of terminals. In the first scenario, we consider a multicast system with 10 terminals and S is set to 60. The corresponding simulation results are plotted in Fig. 5. Both traditional and proposed multicast satisfy the QoS requirements of terminals, which unicast fails to satisfy. It can be observed that our proposed method is more energy efficient than other considered methods. And the energy efficiency is improved with the increase of the maximum transmission power. Similar to homogeneous networks, here we also observe from Fig. 5 that the increment of the maximum transmission power is not equivalent to the decrement of the energy consumption of terminals. Specifically, the quantitative relationship between the maximum transmission power and the terminal energy consumption decrement of the proposed method over traditional multicast is listed in Table V. It can be seen that with the maximum transmission power increases gradually

in steps of 2w starting from 12w, the energy consumption decreasing ratio of the proposed method over the traditional method ranges from 13.795% to 19.543%. And the decreasing ratio diminishes with the increase of the maximum transmission power, which is in accord with Fig. 5.

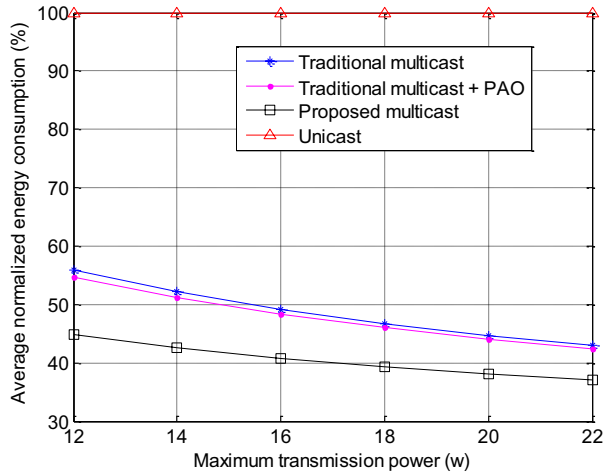


Fig. 5. Energy consumption comparison with different maximum transmission power in heterogeneous networks

TABLE V
THE TERMINAL ENERGY CONSUMPTION DECREMENT OF THE PROPOSED METHOD OVER TRADITIONAL MULTICAST IN HETEROGENEOUS NETWORKS

Maximum transmission power (w)	The terminal energy consumption decrement
12	19.543%
14	18.286%
16	17.087%
18	16.000%
20	14.861%
22	13.795%

In this scenario, we also calculate the marginal terminal energy consumption decrement with successive and fixed increase of the transmission power for the proposed method, which is listed in Table VI. It can be seen that the terminal energy consumption decreases 2.2209%~5.1681% every time the maximum transmission power increases 16.667% in the considered range. Here it is also obvious that from the perspective of terminal energy consumption, the marginal effect brought by the maximum transmission power gets smaller with the increase of the maximum transmission power.

TABLE VI
THE MARGINAL TERMINAL ENERGY CONSUMPTION INCREMENT OF THE PROPOSED METHOD IN HETEROGENEOUS NETWORKS

The marginal increment of the maximum transmission power	The marginal terminal energy consumption decrement
0	0
16.667%	5.1681%
16.667%	4.0960%
16.667%	3.3645%
16.667%	2.6682%
16.667%	2.2209%

In the second scenario, the maximum transmission power is set to 16W and S is set to 60. The effects of the number of terminals are investigated. The corresponding simulation results are plotted in Fig. 6. Here unicast also fails to satisfy the QoS requirements of terminals when $N \geq 5$. And we can derive the same conclusions as homogeneous networks about the effect of the number of terminals on the performance of the proposed method. In the third scenario, the maximum transmission power is also set to 16W and the number of terminals N is set to 10. The effects of S on the energy consumption of terminals are plotted in Fig. 7, where unicast fails to satisfy the QoS requirements of terminals during the considered numbers of symbols. Here it can be also observed that the advantage of the proposed multicast over traditional multicast increases with S, which is in accordance with that in homogeneous networks.

Note that compared to the proposed multicast, there is no optimization on the subcarrier allocation in "traditional multicast+PAO". The simulation results of Fig. 2~7 reveal that subcarrier allocation provides much more contribution than power allocation in reducing the energy consumption of terminals.

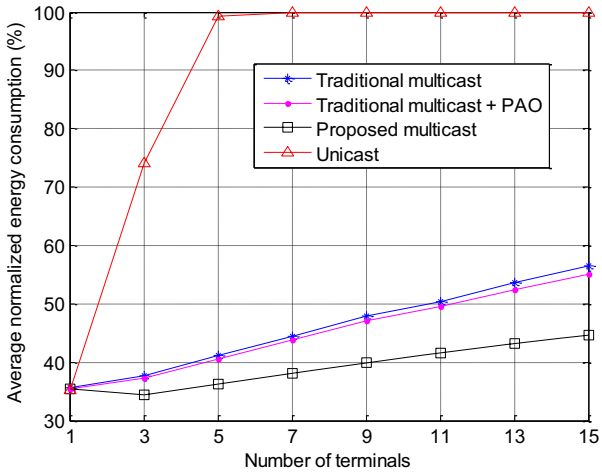


Fig. 6. Energy consumption comparison with different number of terminals in heterogeneous networks

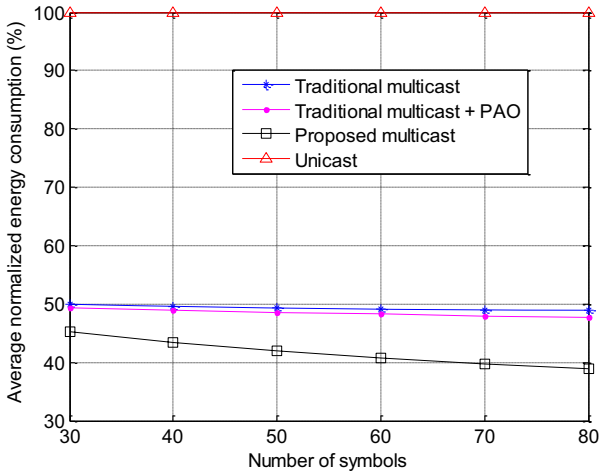


Fig. 7. Energy consumption comparison with different number of OFDM symbols in an OFDMA frame in heterogeneous networks

V. CONCLUSIONS

In this paper, we investigate the energy efficiency of OFDMA-based multicast system from the perspective of terminals in frequency-selective channels. The energy efficiency of terminals is optimized through combining resource allocation with terminal sleep model. A low-complexity algorithm is proposed to solve the formulated optimization problem. The simulation results show that in both homogeneous and heterogeneous networks, the combination of resource allocation and terminal sleep model can reduce the energy consumption of terminals compared to traditional multicast and unicast significantly. Specifically, the terminal energy consumption decreases 2.4110%~6.2884% / 2.2209%~5.1681% every time the maximum transmission power increases 20% / 16.667% compared to the initial value of 1w / 12w in the considered homogeneous / heterogeneous networks. And in the two scenarios, from the perspective of terminal energy consumption, the marginal effect brought by the maximum transmission power gets smaller with the increase of the maximum transmission power. Moreover, the advantage of the proposed multicast over traditional multicast increases with the number of multicast terminals as well as the number of OFDM symbols in an OFDMA frame. Additionally, it indicates that subcarrier allocation contributes much more to the reduction of the energy consumption than power allocation.

REFERENCES

[1] R. O. Afolabi, A. Dadlani, K. Kim, "Multicast Scheduling and Resource Allocation Algorithms for OFDMA-Based Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol.15, no.1, pp.240-254, 2013.

[2] K. Bakanoglu, W. Mingquan, L. Hang, and M. Saurabh, "Adaptive resource allocation in multicast OFDMA systems," *in Proc. IEEE Wireless Communications and Networking Conference (WCNC'10)*, pp. 1–6, Apr.2010.

[3] J. Liu, W. Chen, Z. Cao, and K. B. Letaief, "Dynamic Power and Sub-Carrier Allocation for OFDMA-Based Wireless Multicast Systems," *in Proc. IEEE International Conference on Communications (ICC'08)*, pp. 2607-2611, May 2008.

[4] X. Zhao and S. Jha, "Flexible resource allocation for multicast in OFDMA based wireless networks," *in Proc. IEEE Conference on Local Computer Networks (LCN'12)*, pp. 445-452, Oct. 2012.

[5] C. Tan, T. Chuah, S. Tan, et al., "Efficient clustering scheme for OFDMA-based multicast wireless systems using grouping genetic algorithm," . *Electronics letters*, vol. 48, no. 3, pp. 184-186, 2012.

[6] C. Suh and J. Mo, "Resource allocation for multicast services in multicarrier wireless communications," *IEEE Trans. Wirel. Commun.*, vol.7, no. 1, pp. 27-31, Jan. 2008.

[7] Y. Yu, P. Hsiu, and A. Pang, "Energy-Efficient Video Multicast in 4G Wireless Systems," *IEEE Trans. Mobile Computing*, vol.11, pp. 1508-1522, Oct. 2012.

[8] A. Lina and D. Zaher, "Energy-aware resource allocation in OFDMA wireless multicasting networks," *in Proc. IEEE International Conference on Telecommunications (ICT'12)*, pp. 1–5, April 2012.

[9] 3GPP TS 36.300 v.11.5.0, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2," April 2013.

[10] Y. Ma, K. Letaief, Z. Wang, R. Murch, and Z. Wu, "Multiple description coding-based optimal resource allocation for OFDMA multicast service," *in Proc. IEEE Global Communications Conference (GLOBECOM'10)*, pp. 1–5, Dec. 2010.

[11] S. Deb, S. Jaiswal, and K. Nagaraj, "Real-Time Video Multicast in WiMAX Networks," *in Proc. IEEE International Conference on Computer Communications (INFOCOM'08)*, pp. 2252-2260, April 2008.

[12] Q. Qu and U. C. Kozat, "On the Opportunistic Multicasting in OFDM Based Cellular Networks," *in Proc. IEEE Int. Conf. Commun. (ICC'08)*, Beijing, China, pp.3708-3714, May 2008.

[13] 3GPP TS 25.346 V11.0.0,"Introduction of the Multimedia Broadcast/Multicast Service (MBMS) in the Radio Access Network (RAN); Stage 2," Sep. 2012.

[14] ITU-R Recommendation M.1225, "Guidelines for evaluation of radio transmission technologies for IMT-2000," 1997

[15] J. Liu, Y. Zhang, and J. Song, "Energy Saving Multicast Mechanism for Scalable Video Service Using Opportunistic Scheduling," *IEEE Trans. Broadcasting*, vol. 60, no. 3, pp.464-473, Sep. 2014.

Jun Liu received the B. E. and M. S. degrees in communication engineering from Harbin Institute of Technology, China, in 2008 and 2010, respectively, and the Ph.D. degree in information and communication engineering from Tsinghua University, China, in 2014. From 2014 to 2015, he worked as an engineer at State Grid Information & Telecommunication Branch, Beijng, China. Now he is working as a Postdoctoral researcher at China Academy of Railway Science, Beijing, China. His current research interests mainly include wireless multimedia transmission, energy-efficient scheduling and resource allocation, and big data. He has published more than 10 peer-reviewed journal and conference papers.

Innovation, Convergence and the Disenfranchised: Investigating the Inclusiveness of Convergence in Malaysia

Kamarulzaman Ab. Aziz*,

*Faculty of Management, Multimedia University, Persiaran Multimedia, Cyberjaya 63100, Selangor, Malaysia

kamarulzaman.aziz@mmu.edu.my

***Abstract*—This study proposes to explore the level of inclusive innovation adoption in converged telecommunications as perceived by industry players in Malaysia as well as their attitudes towards the idea using Ajzen's theory of planned behavior (TPB). The paper shares the findings of the pilot study conducted in a focus group of Malaysian telecommunications industry players. Discussions on the robustness of the tool developed, some descriptive statistics, preliminary findings and recommendations for the communications sector are given as well as implications for next stages of the work. In general, the findings indicated that the Malaysian communications industry players moderately agreed on the inclusiveness of the convergence goods currently available in the markets. However, the findings also indicated more can be done to enhance the level of inclusiveness. Furthermore, there appear to be certain differences in attitude towards inclusive innovation according to gender and generation.**

***Keyword*—Convergence, Disenfranchised, ICACT2016, Inclusive, Innovation**

I. INTRODUCTION

Recent years have seen increasing pressure for better ways for tackling poverty problems around the globe beyond aids and charity [1, 2, 3]. The discussions also have highlighted the need for the roles of the torch bearers to go beyond government agencies and NGOs [1 – 7]. Studies by [7] and [8] underlined the significance as 4 billion of the global population was those at the base of the economic pyramid (BOP) and together they represent a potential market of tremendous purchasing power; around $5 trillion. Furthermore, the UN System Task Team formed in September 2011 to support the UN system-wide preparations for the post-2015 UN development agenda, proposed bridging the technological divide by promoting inclusive innovation [9]. These imperatives had underlined the importance and relevance of inclusive innovations towards inclusive growth and the achievement of inclusive societies.

In [10] (p.663) inclusive innovation defined as "the development and implementation of new ideas which aspire to create opportunities that enhance social and economic wellbeing for disenfranchised members of society." According to [11], disenfranchisement or marginalization can be due to economy, state and family as well as along dimensions such as gender, race, disability, knowledge and poverty. Meanwhile, the Global Research Alliance defined inclusive innovation as "any innovation that leads to affordable access of quality goods and services creating livelihood opportunities for the excluded population, primarily at the base of the pyramid, and on a long term sustainable basis with a significant outreach" [12].

Studies of inclusive innovation have previously explored types of organizations and their success strategies [1, 13 – 15]; roles of individuals in organizations [16]; roles of regulation, policy and infrastructures [17]. There seems to be limited studies in terms of inclusive innovation adoption among academic researchers.

In line with the seminal work by [7]; recognizing the sheer size of the market at the bottom of the pyramid, there had been numerous examples of inclusive innovation initiatives by the industries, including Nestle [18], Nokia and ABB [19], Unilever and Tata Motors [10]. In terms of the geography of the inclusive movement the coverage is largely from the African continent [10, 20], South America [21], India [22 – 24], Europe [22, 25], China and North America [22]. A gap clearly exists in the body of knowledge relating to inclusive innovation movement in the Malaysian context.

Wu highlight the importance for inclusive growth towards ensuring ASEAN countries economic development [26], and the Malaysian government specifically recognized the importance of inclusive growth with both innovation and inclusive development identified among the "10 Big Ideas" listed in the 10th Malaysia Plan. In the 10th Malaysia Plan, the government spelled out the move towards inclusive socio-economic development by elevating the livelihoods of the bottom 40% households, strengthening bumiputera entrepreneurs, improving infrastructure, etc. According to the World Bank's country overview report on Malaysia [27], "pockets of poverty exist and income inequality remains high relative to the developed countries Malaysia aspires to emulate". Furthermore, the Malaysian government allocated MYR 5.9 billion in 2016 from MYR 4.6 billion in the 2014 budget for the financial assistance scheme (BR1M) targeting the low income groups [28, 29]. Perhaps the scheme would be

Manuscript received March 15, 2016. This work was supported in part by the Malaysian Ministry of Higher Education under the Fundamental Research Grant Scheme 2014.

Kamarulzaman Ab. Aziz is with the Faculty of Management, Multimedia University, Cyberjaya 63100, Selangor, MALAYSIA (phone: 603-8312-5686; fax: 603-8312-5590; e-mail: kamarulzaman.aziz@ mmu.edu.my).

more effective if there are inclusive innovation goods and services available in the markets for the recipients to purchase.

Another major trend observed currently, is in the communication sector, where computing, ICTs, communication networks, and media content are becoming increasingly highly interlinked. This trend has led to all aspects of life increasingly being conducted over interactive digital media environment and multitude of networked devices.

[30] (p.18-19) highlighted; "Convergence requires media companies to rethink old assumptions about what it means to consume media, assumptions that shape both programming and marketing decisions. If old consumers were assumed to be passive, the new consumers are active. If old consumers were predictable and stayed where you told them to stay, then new consumers are migratory, showing a declining loyalty to networks or media. If old consumers were isolated individuals, the new consumers are more socially connected. If the work of media consumers was once silent and invisible, the new consumers are now noisy and public."

According to [31], convergence can be view from four dimensions;

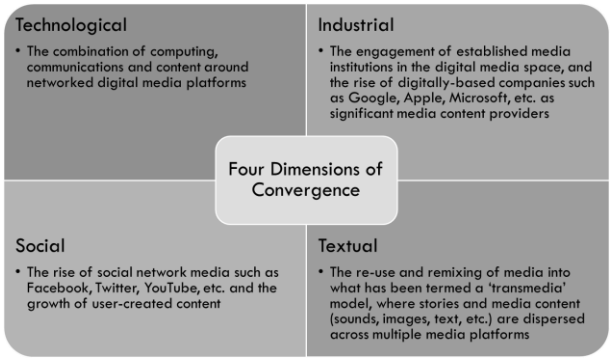


Fig. 1. Four Dimensions of Convergence.

Caution is needed in terms of how the trend is framed - digital lifestyle, modern family, the new consumer, etc. - as there is a real risk of the convergence evolution being non-inclusive. If convergence ends up a privilege enjoyed by the sophisticated, urban and IT haves, the effects of technological/digital divide will be more severe, disenfranchising more among the society and placing a nation's development as a whole at risk.

Thus, this study propose to explore the level of inclusive innovation adoption in converged telecommunications as perceived by industry players in Malaysia as well as their attitudes towards the idea using Ajzen's theory of planned behavior (TPB). TPB was developed by Ajzen in 1988 and later refined in subsequent works [32 – 34]. The theory of planned behavior is a theory which predicts deliberate behavior, because behavior can be deliberative and planned. The theory proposes a model which can measure how human actions are guided. It predicts the occurrence of a particular behavior, provided that behavior is intentional. The model outlines three variables which the theory suggests will predict the intention to perform behavior. The variables are attitudes (Att) - the respondents' attitudes towards inclusive innovation, subjective norms (SN) - the respondents own estimate of the social pressure to adopting inclusive innovation, specifically; beliefs about how other people, who may be in some way important to them, would like them to behave, and perceived behavioral controls (PBC) - is the extent to which the respondents feel able to enact the adopting inclusive innovation behavior. The intentions (Int) are the precursors of behavior, in other words, it is the cognitive representation of a respondents' readiness to adopting inclusive innovation, and it is considered to be the immediate antecedent of behavior.

II. Research Design

This study comprised of several stages. First a group of executives from major telecommunication companies and agencies were solicited to take part in the study. Next, the group was given an exposure to the various aspects of convergence via a series of masterclasses. They were then introduced to the concept of inclusive innovation. Next, each participant was asked to consider the various convergence products/services being offered in the markets and evaluate its inclusiveness. The measure for this is the inclusive innovation index (III), developed from operationalizing the definition of inclusive innovation by the Global Research Alliance. Inclusive innovations are defined along the lines of five dimensions [12]:

- Affordable Access (AA) – "Such inclusive innovation will have to be aimed at `extreme reduction' in both the costs of production as well as the distribution." Key elements for this dimensions are; l) significant reduction of production costs to enable affordable price, and ll) significant reduction of distribution costs to enable affordable price.
- Sustainable Business (SB) – "This means that in the long term, the 'affordable access' must not depend on the government subsidies or generous government procurement support systems but should work by retaining the market principles with which the private sector works comfortably." Thus the key elements are; l) not dependent on government subsidies, ll) not dependent on significant government procurement, lll) not dependent on charity and CSR, and lV) a sustainable business model.
- High Quality (HQ) – "It is because we have to recognize the basic rights of the people at the base of the pyramid, who should be enjoying the more or less the same level of quality of basic services as people at the top of the pyramid." The elements are; l) meeting quality standards, ll) do not sacrifice quality to bring down the costs, and lll) comparable quality level with those of similar products available in the market
- Excluded Population (EP) – "The excluded population or the disenfranchised or commonly marginalized groups which could include the poor, the disabled, the migrants, the women, the elderly, certain ethnic group, and so on." The elements; l) designed for the poor, the disabled, the migrants, the women, the elderly, certain ethnic group, and so on, ll) priced with the poor in mind, and lll) distribution designed to ensure accessibility for the poor, the disabled, the migrants, the women, the elderly, certain ethnic group, and so on.
- Massive Outreach (MO) – "If the `true inclusion' has to

happen then the benefits of inclusive innovation should reach a large scale, i.e. a significant portion of population, and not just a small section of the population (in many cases, the total target population may only be a few hundreds of thousands or a few million- and not necessarily hundreds of million)." The key elements; l) large market size, ll) large market share, and lll) reached sizeable percentage of the target market.

From the five dimensions, based on the definitions and the key elements identified from the definitions, 19 survey items were developed for the III. Following table provide the list of items.

TABLE I
ITEMS FOR INCLUSIVE INNOVATION INDEX

Dimension	Item
AA	• The production costs are significantly low compared to established industrial standard • The distribution costs are significantly low compared to established industrial standard • The products/services are priced affordably low compared to established industrial standard
SB	• The businesses offering the products/services are not dependent on government subsidies • The businesses offering the products/services are not dependent on significant government procurement • The businesses offering the products/services are not dependent on a single major client • The businesses offering the products/services are not dependent on social funding (charity or corporate donations) • There is a long term demand for the products/services • Eventhough the products/services are designed for the commonly marginalized groups it is appealing to the mass market as well
HQ	• The businesses offering the products/services ensures the products/services meet all relevant quality standards • The businesses offering the products/services don't sacrifice quality to bring down the costs • The businesses offering the products/services ensure any cost reduction does not compromise the quality • The products/services' quality is comparable with those of similar but higher priced products available in the market
EP	• The products/services are designed for the commonly marginalized groups such as the poor / bottom 40% / disabled / migrants / women / elderly / minority groups / etc • The products/services are priced affordably; with the poor / bottom 40% in mind • The distribution channels are designed/selected to ensure the products/services are accessible by the commonly marginalized groups such as the poor / bottom 40% / disabled / migrants / women / elderly / minority groups / etc
MO	• There is a large market potential for the products/services • The products/services already have a large share of the target market • The products/services have reached more than 50% of the target market

Their intention towards inclusive innovation is then gauged via a survey develop based on Ajzen's TPB. The findings are presented in the following sections.

III. FINDINGS

A total of 30 executives took part in the study. Among them, 17 (56.7%) were males while the remaining 13 (43.3%) were females. The age ranged from 20-24 to 45-49 years old. Out of the 30, 12 (40%) have Master degrees, and 18 (60%) have Bachelor degrees. The participants had a mean of 9.43 years work experience with their current organization, ranging from first year to the 22nd year. Furthermore, 29 (96.7%) of them claimed that their organization do their own R&D and product development.

Reliability analysis was conducted to determine the internal reliability of the items used to measure the constructs tested in this study. According to [35], Cronbach's Alpha is a reliability coefficient that indicates the extent to which the items are positively correlated to one another. Cronbach's Alpha greater than 0.70 is deemed as good [36]. All of the constructs were considered as reliable and good as the Cronbach's Alpha were above 0.70 (see Table II).

TABLE II
RELIABILITY ANALYSIS

Constructs	N	Items Mean	Std. Dev.	Cronbach's Alpha	No. of Items
Att	30	4.272	12.70754	0.982	6
SN	30	5.258	4.55982	0.722	4
PBC	30	4.775	4.49022	0.729	4
Int	30	5.725	4.95044	0.926	4
III	30	5.174	10.87278	0.802	19

A total of 37 items were used to measure the main constructs of the study, namely III (19 items), Att (6 items), SN (4 items), PBC (4 items) and Int (4 items). The items were measured by itemized rating scale with seven scale categories. Mean analysis was conducted to determine the average mean of the constructs.

Generally, the respondents agreed with all the items measuring the constructs with overall Int achieved the highest level of agreement with an average of 5.7250 and median of 6.000; while overall Att scored the lowest with an average of 4.2722 and median of 4.7500. Meanwhile, overall PBC achieved a mean of 4.7750 and median at 4.500. Overall SN achieved the second highest mean of 5.2583 and median at 5.1250. The respondents rated a moderate level of agreement on inclusiveness of convergence goods currently available in the markets with overall III of 5.1737 and median at 5.2895, suggesting that there is still the need to produce more inclusive convergence goods. The overall Int mean being the highest gives a good indication of the industry players in Malaysia intending to adopt inclusive innovation when developing goods and services for their customers in the future.

The above was further confirmed when each participant was asked whether they think that it is important for the industry to develop inclusive convergence goods and services, with a mean of 6.03 and median at 6.0. The group also agrees that such goods or services can also be appealing to the mass market (mean 5.13 and median 6.0). The group in general reported being unable to identify specific inclusive convergence goods or services or policies specifically designed to promote the development of such goods (mean

4.73 and 5.13 respectively).

Comparing the means between the male and female participants shows some marked difference in their overall attitude towards inclusive innovation with the male participant showing a lower mean than female suggesting less than favorable attitude towards inclusive innovation in the context of their industry. However, when asked on their intention to adopt inclusive innovation in their business (the participants were asked to assume that they have the authority to decide), both gender recorded higher mean from their initial attitude, with male executives recording higher intention than their females colleagues.

The respondents were regrouped into two generations – younger (10, 33.3%) and older (20, 66.7%) – with the age 35 years old being the threshold age. Similar comparative analysis done according to gender earlier was carried out according to the generations. There are some marked differences between the two groups with the younger generation recording higher means for attitude, subjective norms and intention. On the other hand, the older recorded higher means for PBC and III. See Table III below for the full means comparison.

TABLE III
COMPARING MEANS

Constructs	Male	Female	Younger	Older
Overall III	5.1796	5.1661	5.0526	5.2343
Overall Att	3.7549	4.9487	4.4333	4.1917
Overall SN	5.1324	5.4231	5.4750	5.1500
Overall PBC	4.8529	4.6731	4.6750	4.8250
Overall Int	5.8235	5.5962	5.9500	5.6125

The comparative analysis was also conducted in terms of how the groups responded on the questions on i) whether they think that it is important for the industry to develop inclusive convergence goods and services, ii) whether such goods or services can also be appealing to the mass market, iii) ability to identify specific inclusive convergence goods or services, and iv) ability to identify policies specifically designed to promote the development of such goods.

The female respondents in general recorded higher means on all four questions than their male counterparts. The younger respondents of the group recorded higher means on the first two questions than their older colleagues and the pattern was flipped on the last two questions, with the older group recorded higher means. See following Table IV for the full means comparison.

TABLE IV
COMPARING MEANS

Constructs	Male	Female	Younger	Older
Important	6.0000	6.0800	6.4000	5.8500
Mass Market	4.9400	5.3800	5.5000	4.9500
Goods/Services	4.4700	5.0800	4.4000	4.9000
Policies	5.1200	5.1500	5.0000	5.2000

IV. DISCUSSIONS

The findings indicated that the Malaysian communications industry players moderately agreed on the inclusiveness of the convergence goods currently available in the markets. However, when asked further, the participants largely unable to identify specific goods and policies for the production of inclusive convergence goods. Thus, the earlier moderate agreement might be more of an optimistic and hopeful perception on the side of the participants. The findings also showed positive indications towards inclusive innovations among the participants where the group showed a good level of agreement on the importance and potential of inclusive convergence goods and services. Even though, when considering inclusive innovations in the context of their businesses, the participants showed poor attitude towards it, they then reported more positive response in terms of intention to adopt inclusive innovations if the authority to take the decision is theirs. This suggests that more exposure and promotions need to be done by the government to increase the level of awareness and understanding of inclusive innovations within the industry. Development of inclusive convergence communications goods and services should be incentivized, with success stories being shared and celebrated. The Inclusive Innovation Index (III) developed for this study serves as a useful tool that can be used to help get this movement under way.

The differences observed in the responses between the genders and generations suggest there most likely different appreciations and behaviors towards inclusive innovation according to gender and age. This hypothesis seems to be supported by some previous reports and researches. In the Mobile Behavior Report 2014 by Salesforce Inc. [37], in terms of gender, females were ahead of males in smartphone ownership. Similar differences were reported in reports by CEOWORLD Magazine in 2014 [38] and by Intel in 2013 [39], where females were reported to lead in;

- installing mobile apps
- purchasing apps
- willingness to pay more for the apps
- playing mobile games.

Furthermore, according to a report by Deloitte in 2014 [40], the older generations in developed countries showed significant growth in smartphone ownership and high mobile apps download rate. However, in a report by Pew Research Centre also in 2014 [41], IT adoption rate among the older generation was still lagging behind that of the younger generations. Furthermore, studies have shown that the younger generations tend to have higher self-efficacy in IT [42].

However, it is not possible to deduce conclusively on the differences among gender and age groups based on the findings of this study due to the small sample size.

Next, this study should be implemented with a larger sample size in order to gain better insights to the true state. The design of the research project would need to be refined for practical purposes. The masterclasses would be hard to be replicated when dealing with larger sample size. Thus, the content from the masterclasses need to be condensed and presented in formats that would suit a survey study. It is

proposed that a short informative tutorial video is produced which can be included as the introductory portion of the online survey. A textual version should also be produced and presented as leaflets to be provided along with the paper-based survey. The survey participants should include all stakeholder groups of the communications sector. Differences in the findings among the different stakeholder groups should be explored and implications discussed to generate comprehensive recommendations.

V. CONCLUSIONS

The convergence trend will continue to be the major driving trend in the communications sector. The trend is fueled by rapid development of various related technologies, which then spur more innovative sparks that will continue to take the trend into wider aspects of human lives.

Innovation capacity is thus the critical factor for organizations to ensure their continued performance and competitiveness. Malaysian organizations need to develop their ability to become global trailblazers; not to be complacent and satisfied to only follow global trends, nor banking on continued government protection of domestic players.

It is important to recognize the directions the convergence evolution is taking and to plan for the various infrastructure as well as policy needs. Readiness is crucial in order to be in step with the technological progress and market expectations.

The findings from this study suggest differences in attitude towards inclusive innovation may exist due to gender and age. However, the findings from this study are not sufficient for a conclusive argument. What is clear is that such lines of investigations are worth exploring and may bear some interesting findings. Comparison between the generations should be expanded beyond the simplistic division of young and old. Generation X, Y and millennials may behave and perceive inclusive innovation differently.

Furthermore, caution is needed in terms of how we frame the trend. Digital lifestyle, modern family, the new consumer, etc.; there is a risk of making the convergence evolution non-inclusive.

If convergence ends up a privilege enjoyed by the sophisticated, urban and IT haves, the effects of technological/digital divide will be more severe, disenfranchising more among the society and may put the nation's development as a whole at risk.

Some may still argue that ensuring inclusion is not the responsibility of the private sector. However, earlier studies have argued it otherwise. Armed with insights provided from studies such as this, ensuring the inclusiveness of convergence should be an agenda promoted by the government and implemented by the industry.

ACKNOWLEDGMENT

This study was made possible by the Fundamental Research Grant Scheme (FRGS) from the Ministry of Higher Education, Malaysia.

REFERENCES

[1] C. K. Prahalad, *The Fortune at the Bottom of the Pyramid, Revised and Updated 5th Anniversary Edition: Eradicating Poverty Through Profits*. 1st ed., Pearson FT Press, 2009.
[2] C. K. Prahalad, and A. Hammond, "Serving the world's poor profitably," *Harvard Business Review*, vol. 80, pp. 48-57, 2002.
[3] UNDP, *Creating value for all: strategies for doing business with the poor. Report of the growing inclusive markets initiative.* New York, 2008.
[4] S. Hart, *Capitalism at the crossroads: The unlimited business opportunities in serving the world's most difficult problems.* Upper Saddle River, NJ: Wharton School Publishing, 2005.
[5] P. Kandachar, and M. Halme, "Farewell to pyramids: how can business and technology help to eradicate poverty." in [5] P. Kandachar, and M. Halme (Eds) *Sustainability challenges and solutions at the base of the pyramid: Business, technology and the poor*. London: Greenleaf. pp. 1-28, 2008.
[6] S. Srinivasa, and J. Sutz, "Developing countries and innovation: searching for a new analytical approach." *Technology in Society*, vol. 30. pp. 129-140, 2008.
[7] C. K. Prahalad, and S. Hart, "The fortune at the bottom of the pyramid." *Strategy+Business*. Vol. 26, pp. 1-13, 2002.
[8] World Resources Institute, *The Next 4 Billion: Market Size and Business Strategy at the Base of the Pyramid*. Washington, 2007.
[9] United Nations Available: http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/28_thinkpiece_science.pdf, Aug. 2014.
[10] G. George, A. M. McGahan, and J. Prabhu, "Innovation for inclusive growth: Towards a theoretical framework and a research agenda." *Journal of Management Studies*. 49 (4), pp. 661 – 683, 2012.
[11] M. Burton and C. Kagan, "Marginalization." in G. Nelson and I. Prilleltensky, (Eds). *Community psychology: in pursuit of wellness and liberation*. London, Palgrave Macmillan, 2005.
[12] Global Research Alliance, "Inclusive Innovation." Available: http://theglobalresearchalliance.org/en/What-we-do/Inclusive-Innovation.aspx, Dec. 2012.
[13] J. Anderson, and C. Markides, "Strategic innovation at the base of the economic pyramid." *MIT Sloan Management Review*, vol. 49. pp. 83-88, 2007.
[14] R. Galema, R. Lensink, and R. Mersland, "Do powerful CEOs determine microfinance performance?" *Journal of Management Studies*, vol. 49. pp. 718-742, 2012.
[15] R. M. Kanter, "Transforming giants." *Harvard Business Review*, vol. 86. pp. 43-52, 2008.
[16] P. Tracey, N. Phillips, and O. Jarvis, "Bridging institutional entrepreneurship and the creation of new organizational forms: a multilevel model." *Organization Science*, vol. 22. pp. 60-80, 2011.
[17] J. Hall, S. Matos, L. Sheehan, and B. Silvestre, "Entrepreneurship and innovation at the base of the pyramid: a recipe for inclusive growth or social exclusion?" *Journal of Management Studies*, vol.49. pp. 785-812, 2012.
[18] Nestle Research, *Popularity positioned products: Affordable and Nutritious*. Renens: Nestec SA, 2011.
[19] M. Halme, S. Lindeman, and P. Linna, "Innovation for Inclusive Business: Intrapreneurial Bricolage in Multinational Corporations." *Journal of Management Studies*, vol. 49, pp.743–784, 2012.
[20] J. Khayesi, and G. George, "When does the socio-cultural context matter? Communal orientation and entrepreneurs' resource accumulation efforts in Africa." *Journal of Occupational and Organizational Psychology*, vol. 84. pp. 471-492, 2011.
[21] A. Smith, M. Fressoli, and H. Thomas, "Grassroots innovation movements: challenges and contributions." *Journal of Cleaner Production*. pp. 1-11, 2013.
[22] R. Rezaie, A. M. McGahan, S. Frew, A. Daar, and P. Singer, "Biopharmaceutical innovation in China, India, Brazil and South Africa: Implications for the United States." Working paper. University of Toronto, 2011.
[23] L. Sonne, "Innovative initiatives supporting inclusive innovation in India: Social business incubation and micro venture capital." *Technological Forecasting & Social Change*, vol. 79. pp. 638-647, 2012.
[24] S. Ramani, and V. Mukherjee, "Can breakthrough innovations serve the poor (bop) and create reputational (CSR) value? Indian case studies." *Technovation*, vol. 34. pp. 295-305, 2014.
[25] D. L. T. Hegger, G. Spaargaren, B. J. M. van Vliet, and J. Frijns, "Consumer – inclusive innovation strategies for the Dutch water supply sector: Opportunities for more sustainable products and

services." *NJAS-Wageningen Journal of Life Sciences*, vol. 58. pp.49-56, 2011.
[26] D. Wu, Rethinking the development gap: ASEAN's inclusive growth imperative. Available: http://thediplomat.com/2013/05/rethinkingthe-development-gap-aseans-inclusive-growth-imperative/?allpages=yes&print=yes, Dec. 2013.
[27] World Bank, Malaysia Overview (Updated on February 28, 2014). Available: http://www.worldbank.org/en/country/malaysia/overview.print, 2014.
[28] MyBajet, Bajet 2014, Available: http://mybajet.my/budget-2014-full-text-of-prime-ministers-speech, Aug. 2014.
[29] The Sun Daily, BR1M increased under Budget 2016, Available: http://www.thesundaily.my/news/1591875, Nov. 2015.
[30] H. Jenkins, *Convergence Culture: Where Old and New Media Collide*, New York: New York University Press, 2006.
[31] G. Meikle and S. Young, *Media Convergence: Networked Digital Media in Everyday Life*, London: Palgrave Macmillan, 2012.
[32] I. Ajzen, *Attitudes, Personality, and Behavior*. Chicago, IL.: Dorsey Press, 1988.
[33] I. Ajzen, "Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179 – 211, 1991.
[34] I. Ajzen, Constructing a TpB Questionnaire: Conceptual and Methodological Considerations. 2006. Available: http://www.people.umass.edu./aizen/pdf/tpb.measurement.pdf, March. 2010.
[35] U. Sekaran, *Research Methods for Business: A Skill Building Approach*, New York: Wiley, 2000.
[36] N. L. Leech, K. C. Barrett, and G. A. Morgan, *IBM SPSS for Intermediate Statistics: Use and Interpretation*, 4th ed, London: Routledge, 2011.
[37] Salesforce Inc., 2014 Mobile Behavior Report, Available: http://www.exacttarget.com/sites/exacttarget/files/deliverables/etmc2014mobilebehaviorreport.pdf, October. 2014.
[38] CEOWORLD Magazine, Gender differences in social media and mobile use, Available: http://ceoworld.biz/ceo/2014/04/09/gender-differences-in-social-media-and-mobile-use-99209834, December. 2014.
[39] Intel, The Gender App: What's the Difference? 2013. Available: https://software.intel.com/en-us/blogs/2013/04/30/the-gender-app-what-s-the-difference, October. 2014.
[40] Deloitte, The smartphone generation gap: over 55? There's no app for that, Available: http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-2014prediction-smartphone.pdf, October. 2014.
[41] Pew Research Centre, Seniors and Tech Use, Available: http://www.pewinternet.org/files/2014/04/PIP_Seniors-and-tech-use_040314.pdf, October. 2014.
[42] Y. S. Wang, M. C. Wu, and H. Y. Wang, "Investigating the Determinants and Age and Gender Differences in the Acceptance of Mobile Learning." *British Journal of Educational Technology*, vol. 40, pp. 92-118, 2009.

Kamarulzaman Ab. Aziz is currently an associate professor and the Director of the Entrepreneur Development Centre at Multimedia University, member of the Centre of Excellence for Business Performance (CeBP) and the Centre for Knowledge & Innovation Management (CEKIM), and was the Deputy Dean (R&D) of the Faculty of Management, Multimedia University. He was also the founding president of the AKEPT Young Researchers Circle (AYRC). His research interest includes Cluster Development, Technology and Innovation Management, Entrepreneurship and Commercialization.

Performances of Polar Codes in Steganographic Embedding Impact Minimization

Birahime Diouf, Idy Diop, Sidi Mohamed Farssi

Department of Computer Science, Polytechnic Institute (ESP) / Cheikh Anta Diop University (UCAD), Dakar, Senegal

dioufbira11@yahoo.fr, idydiop@yahoo.fr, farsism@yahoo.com

***Abstract*—Syndrome coding is used in practice by many authors to define steganographic schemes that minimize embedding impact. Polar Codes, recently introduced, are the first capacity-achieving codes with low complexity of encoding and decoding. In this paper we propose a new practical polar coding methodology for constructing steganographic scheme. We use syndrome coding with binary embedding operation. The approach exploits the form of the syndrome, calculated from cover and secret message. A connection between the syndrome decimal value and the embedding changes position is established and enables defining a new steganographic algorithm. The wet paper codes can also be implemented using this method. Experimental results prove that the scheme minimizes the embedding impact with a reduced time complexity compared to the first Polar Coding Steganography (PCS). The bit-reversal permutation matrix used in polar coding is also employed in practice to uniformly scatter the changes over the whole image.**

***Keywords*—Embedding impact, matrix embedding, polar code, steganography, wet paper codes.**

I. INTRODUCTION

THE steganography is an information hiding technique that enables to conceal a message in a cover medium x in such a way that it existence is kept secret [1]. The cover medium can be digital media such as an image (used in this paper), a sound or a video. The steganalysis aims to detect the existence of secret message. The sender, known as *steganographer* [2], should embed her covert communication or *payload* in a cover medium in such a way that only the receiver is aware of the existence of secret communication. The receiver can extract the messages without being aware of the sender choices. Steganography have both good and evil uses.

The embedding must be done by making the cover medium changes less noticeable as possible. In spatial domain, the bits of secret message can be inserted at the LSBs (Least Significant Bits) of the cover image pixels. To improve this so called LSB technique, several propositions exist. The most evident is (a): to make less changes as possible and (b): so that they were less detectable. To answer the first problem of minimizing the number of changes (a), Crandall introduced and conceptually described a steganographic technique [3]. A connection between codes and the problem of minimizing the number of changed pixels (the constant profile) is established by Bierbrauer [4].The first implementation of this technique was created with the F5 algorithm of Westfeld [5] in which the Hamming codes were used. Afterwards, several schemes have implemented this technique in steganography using Golay [6], BCH (Bose-Chaudhuri- Hocquenghem) [7], [8], LDGMs (Low Density Generator Matrices) [9] in combination with the ZZW (Zhang-Zhang-Wang) construction [10], STC (Syndrome Trellis Codes) [11], [12] and LDPC (Low Density Parity Check) [13] codes. The second problem (b) can be solved using wet paper codes [14]. After having introduced polar codes in steganography PCS (Polar Coding Steganography) [15], we propose in this paper a new practical method for minimizing embedding impact with a reduced algorithmic time complexity. It exploits the relation between syndrome decimal value and embedding changes position. The originality of this work lies in defining an algorithm which gives stego medium in a single step compared to PCS [15] and without using lookup tables [16]. Moreover, this new methodology is applied on images in spatial domain. The images are beforehand randomly permuted to scatter the changes over isolated pixels.

This paper is organized as follows. Section II gives a brief review of basic concepts in steganography and polar coding. In Section III, we present PCS scheme. New steganographic scheme is studied in Section IV. Section V provides a time complexity comparison between PCS scheme [15] and the proposed new algorithm [17]. This section shows also the practical results of the permutation of images. Section VI concludes the paper.

II. STEGANOGRAPHY AND POLAR CODES BASIC CONCEPTS

We will denote by $\mathrm{x} = (x_1, \ldots, x_n) \in \mathcal{X} = \{0,1\}^n$ the LSBs of the cover 8-bits grayscale image and x_i its i^{th} LSB in in spatial domain. The secret message $\mathrm{m} = (m_1, \ldots, m_m) \in \mathcal{M} = \{0,1\}^m$ is embedded by slightly modifying the cover image. This create the LSB-stego-image

Manuscript received December 26, 2015. This work is supported by the Laboratory of Medical Imagery and Bioinformatics in Polytechnic Institute, Cheikh Anta Diop University, Senegal, and a follow-up of the invited journal to the accepted out-standing conference paper of the 17th International Conference on Advanced Communication Technology (ICACT2015).

Birahime Diouf is with the Department of Computer Science, Polytechnic Institute, Cheikh Anta Diop University, Dakar, Senegal (Corresponding author, phone: +221 77 220 43 50; fax: +221 8253724; email: dioufbira11@yahoo.fr).

Idy Diop is with the Department of Computer Science, Polytechnic Institute, Cheikh Anta Diop University, Dakar, Senegal (idydiop@yahoo.fr).

Sidi Mohamed Farssi is with the Department of Computer Science, Polytechnic Institute, Cheikh Anta Diop University, Dakar, Senegal (farsism@yahoo.com).

$\mathrm{y} = (y_1, \ldots, y_n) \in \mathcal{Y} = I_1 \times \ldots \times I_n$, where $I_i \subset I$ such that $x_i \subset I_i$. We will use the binary LSB replacement method where $I_i = \{x_i, \overline{x_i}\}$ (cardinality $|I_i| = 2$, for all i), where $\overline{x_i}$ is x_i after flipping its value. We denote by e the embedding change vector ($\mathrm{y} = \mathrm{x} + \mathrm{e}$) and $\mathrm{H} \in \{0,1\}^{m \times n}$ is a parity check matrix of the code.

A. Steganography and Basic Concepts

Matrix embedding is introduced in steganography by Crandall [3] to minimize the number of embedding changes. It is based on syndrome decoding of error correcting codes. Subsequently, several codes are used to implement this technique in steganography.

1) Distortion function:

The embedding impact produced by cancelling the secret message m in the cover vector x will be measured using a distortion function *D*. In this paper, we limit ourselves to an additive distortion [12]

$$D(\mathrm{x}, \mathrm{y}) = \sum_{i=1}^{n} \rho_i(\mathrm{x}, \mathrm{y}_i) \ , \tag{2}$$

where $\rho_i(\mathrm{x}, y_i)$ is the cost of replacing the cover pixel x_i with stego pixel y_i. Note that ρ_i may arbitrarily depend on the entire cover image x. The independency of the value of $\rho_i(\mathrm{x}, y_i)$ to changes made at other pixels implies that the embedding changes do not interact. In others words, the change of a pixel has no effect on the other pixels. In the case of binary embedding operation, the distortion can be written as [11]

$$D(\mathrm{x}, \mathrm{y}) = \sum_{i=1}^{n} \rho_i \left| \mathrm{x}_i - \mathrm{y}_i \right| \tag{3}$$

2) Minimizing embedding impact:

In this paper we use the PLS (Payload-Limited Sender) that that is to embed a fixed average payload while minimizing the average distortion opposed to DLS (Distortion-Limited Sender) that maximize the average payload while introducing a fixed average distortion [12]. The PLS is more commonly used in steganography when compared to the DLS. For a PLS, the sender tries to embed her secret message m so that the total distortion *D* is minimized; that make the resulting stego-system less detectable (more secure). This problem has been approached using variants of syndrome coding [5]–[13]. The sender and the receiver, respectively, implement the embedding and extraction functions $Emb : \mathcal{X} \times \mathcal{M} \to \mathcal{Y}$ and $Ext : \mathcal{Y} \to \mathcal{M}$ satisfying

$$Ext\left(Emb\left(\mathrm{x}, \mathrm{m}\right)\right) = \mathrm{m} \quad \forall \mathrm{x} \in \mathcal{X}, \forall \mathrm{m} \in \mathcal{M}, \tag{4}$$

The embedding is seen as being universal because the distortion function *D* is unknown at the receiver. For a binary linear code $\mathcal{C}$ of length n and dimension $n - m$

$$\begin{aligned} Emb(\mathrm{x}, \mathrm{m}) &= \arg \min_{\mathrm{y} \in \mathcal{C}(\mathrm{m})} D(\mathrm{x}, \mathrm{y}) \\ Ext(\mathrm{y}) &= \mathrm{y}\mathrm{H}^{\mathrm{T}} = \mathrm{m} \end{aligned} \tag{5}$$

where $\mathcal{C}(\mathrm{m}) = \left\{ \mathrm{z} \in \{0,1\}^n \mid \mathrm{z}\mathrm{H}^{\mathrm{T}} = \mathrm{m} \right\}$ is the coset corresponding to syndrome m and all operations are in binary arithmetic. The extraction function is equivalent to

$$Ext(\mathrm{y}) = \mathrm{y}\mathrm{H}^{\mathrm{T}} = \mathrm{m} \leftrightarrow Ext(\mathrm{e}) = \mathrm{e}\mathrm{H}^{\mathrm{T}} = \mathrm{m} - \mathrm{x}\mathrm{H}^{\mathrm{T}}, \tag{6}$$

Then, in constant profile, searching the stego vector y amounts to search the change vector e of minimal weight in the coset $\mathcal{C}(\mathrm{m} - \mathrm{x}\mathrm{H}^{\mathrm{T}})$. Syndrome coding is capacity achieving for the PLS problem if random linear codes are used. Unfortunately, random linear codes are not practical due to the exponential complexity of the optimal binary coset quantizer (4), which is the most challenging part of the problem.

3) Wet Paper Codes:

The wet paper channel is based on pixels selection technique which consists in choosing pixels whose change is less perceptible by human visual system and having less statistical effects on the cover image. In the case where all pixels are assigned $\rho_i = 1$ (the so called constant profile), minimizing the distortion *D* is reduced to minimize the number of embedding changes. However, in practice some pixels of the cover image can be more sensitive to change than others. The first called wet pixels (with $\rho_i = \infty$); we must force the embedding algorithm to keep such pixels unchanged. The second called dry pixels (with $\rho_i = 1$) can be changed. In this case we say that we have a wet paper channel [15]. The syndrome coding is also applied to this type of channel using wet paper codes [11], [12] and [15]. The polar code design for wet paper channel with a given relative wetness $\tau = \left| \{ i : \rho_i = \infty \} \right| / n$, withe $|X|$ denotes the cardinality of the set *X*, is described in Section IV-B.

B. Polar Codes

Based on a new paradigm of coding, polar codes are defined as the first codes that achieve the channel capacity, limit established by Shannon. A polar code of length $n = 2^p$ and dimension *k* will be denoted by *PC*(*n*,*k*). W is a B-DMC (Binary-input Discrete Memoryless Channel). The symmetric capacity [18] of W is denoted by I(W) and the reliability parameter is Z(W). Let A and its A^{c} respectively denote information and frozen bits sets. The construction of polar codes is based on channel polarization. It consists in synthesizing of *n* independent copies of a given B-DMC W to create *n* others channels $\{\mathrm{W}_n^{(i)} : 1 \le i \le n\}$. It is made up two steps: channel combining and channel splitting [18] with we summarize as follows:

$$(\mathrm{W}, \mathrm{W}, ..., \mathrm{W}) \xrightarrow{\text{combining}} \mathrm{W}_n \xrightarrow{\text{splitting}} \left\{ \mathrm{W}_n^{(i)} \right\}_{i=1,\ldots,n} . \tag{7}$$

The channel combining combines *n* copies of a given B-DMC W in a vector channel W_n. It is done recursively by

combining two copies of $W_{n/2}$. During channel splitting we subdivide W_n into n channels $W_n^{(i)}$, $1 \le i \le n$. Channel polarization can be seen as a recursive channel transformation process which can be represented as follows [15], [17]:

$$\left(W_n^{(i)}, W_n^{(i)}\right) \xrightarrow{\text{we construct}} \left(W_{2n}^{(2i-1)}, W_{2n}^{(2i)}\right). \quad (8)$$

The polar coding is done using the following relationships:

$$x_1^n = u_1^n G_n$$
$$G_n = B_n G_2^{\otimes p} = B_n \begin{bmatrix} G_{n/2} & 0 \\ G_{n/2} & G_{n/2} \end{bmatrix}, \quad (9)$$

with B_n is a bit-reversal permutation matrix, G_n is a generator matrix, $u_1^i = (u_1, \ldots, u_i)$, with $1 \le i \le n$ and $G_1 = [1]$ and $G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. The Kronecker product between matrix $A = [A_{ij}]$, $1 \le i \le n$ and $1 \le j \le m$ and $B = [B_{ij}]$, $1 \le i \le q$ and $1 \le j \le r$ is defined by

$$A \otimes B = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{bmatrix} \quad (10)$$

which is a $mq \times nr$ matrix. The Kronecker power is defined by $A^{\otimes p} = A \otimes A^{\otimes (p-1)}$, for all $p \ge 1$, with $A^{\otimes 0} = [1]$.

For polar code *PC(8,4)*, we have:

$$G_2^{\otimes p} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&1&1&1&0&1&1 \end{bmatrix} \text{ and } G_n = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&0&1&0&1&0&1&0 \\ 1&1&0&0&0&0&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&1&0&1&1 \end{bmatrix} \quad (11)$$

The information word u_1^n is transformed in a code word x_1^n. Each bit x_i of x_1^n borrows a copy of W and the gives the bit y_i of the received word y_1^n as shown in Fig. 1.

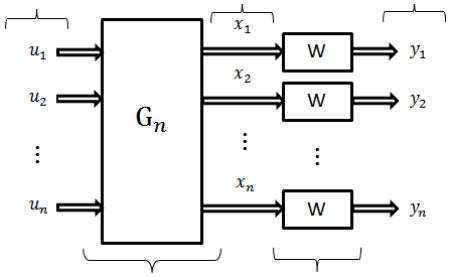


Fig. 1. Polar coding scheme.

In polar coding if u_1^n has a uniform distribution then $W_n^{(i)}$ is the channel really seen by u_i (Fig. 2).

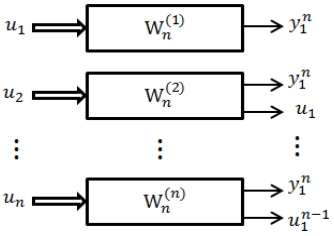


Fig. 2. Equivalent of polar coding scheme.

The most reliable $W_n^{(i)}$ are used to carry the information bits and the least reliable ones contain the frozen bits $Z(W_n^{(i)}) \le Z(W_n^{(j)})$, for any $i \in A$ and $j \in A^c$

Polar codes are several applications in information theory and have been recently introduced in steganography [15].

III. First PCS (Polar Coding Steganography) Method

Denote by $\mathcal{S}_{PC}(n,m=n-k)$ the steganography based on polar code $PC(n,k)$.

A. Construction of Polar Codes in Steganography

The construction of polar codes for the purposes of steganography can be summed up in three steps [15] as shown in Fig. 3.

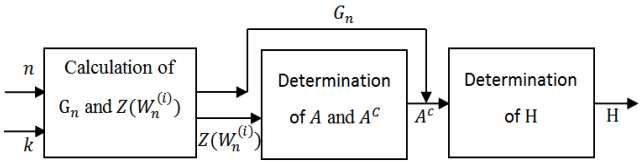


Fig. 3. Construction of polar codes for steganographic purposes.

We calculate the reliability parameters as follows [15]:

$$Z\left(W_n^{(j)}\right) = 2Z\left(W_{n/2}^{((j+1)/2)}\right) - Z\left(W_{n/2}^{((j+1)/2)}\right)^2 \quad \text{if } j \text{ is even}$$
$$Z\left(W_n^{(j)}\right) = Z\left(W_{n/2}^{(j/2)}\right)^2 \quad \text{if } j \text{ is odd} \quad (12)$$

The initial value is calculated with

$$Z\left(W_1^{(1)}\right) = Z(W) = 2\sqrt{W(0|0)W(0|1)} = 2\sqrt{p_e(1-p_e)}, \quad (13)$$

where p_e is the error probability of the channel W, $p_e = W(0|1) = W(1|0)$ and $1 - p_e = W(0|0) = W(1|1)$.

To obtain A and A^c we select channels with the parameters of the lowest reliabilities for data bits. The indices of these channels form the information bits A. Its cardinality is equal to the dimension k of the considered polar code. The $n-k$ other channels carry redundancy bits. Their indices constitute A^c.

To determinate a parity check matrix of a polar code, we use the lemma given by Goela *et. al.* [19, Lemma 1] which states that if the frozen bits are equal to 0 then the transpose of the parity check matrix H of the polar code is given by the columns of the generator matrix G_n whose indices are in A^c.

As examples, we use a polar code *PC(4,1)* for the steganography $\mathcal{S}_{PC}(4,3)$ and *PC(8,4)* for $\mathcal{S}_{PC}(8,4)$.

For *PC(4,1)*, $A = \{4\}$, $A^c = \{1, 2, 3\}$ and a parity check matrix is:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \text{ and its transpose } H^T = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad (14)$$

If we use *PC(8,4)* then $A = \{4, 6, 7, 8\}$, $A^c = \{1, 2, 3, 5\}$ and from (11) we have :

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \text{ and } H^T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad (15)$$

The steganographic scheme is made up two steps.

B. First Step

By making the most of the particular form of H and its transpose H^T, we can transform the equations of the relation $yH^T = m$ in a system allowing calculating the coefficients of the stego vector y (see [15]):

$$y_i = y_{i+1}H^T_{(i+1),j} + \cdots + y_n H^T_{nj} + m_j \; ; j = n-k \text{ down to } 1 \quad (16)$$

with i the position of first 1 on column j of H^T. For each j, we calculate the corresponding y_i. The vector y must be initialized to the cover vector x before the calculations. With (16), we obtain a stego vector y_p verifying $yH^T = m$ but it is not the closest to the cover vector x.

C. Optimization of the First Solution

The objective of this step is to find the stego vector y closest to x by using the polar code *PC(n,k)*. Let e_p be the embedding change vector corresponding to the stego vector y_p found with the first step. The distortion (3) can be written:

$$D(e) = \sum_{i=1}^{n} \rho_i e_i \quad (17)$$

where $|x_i - y_i| = e_i$ and $\rho_i = 1$ for constant profile and $\rho_i = \{1, \infty\}$ for wet paper channels. The insertion and extraction functions become:

$$\begin{aligned} &Emb(x, m) = \arg \min_{e \in C(s)} D(e) \\ &Ext(y) = yH^T = m \Leftrightarrow eH^T = s = m - xH^T \end{aligned} \quad (18)$$

Considering the problem in the following three points [15]:

- we have a first solution $e_p \rightarrow$ initial solution,
- we have to minimize the distortion $D(e) \rightarrow$ minimization problem,
- verifying $eH^T = m - xH^T = s \rightarrow$ constraints,

we have a minimization problem with equalities constraints and initial solution e_p. The problem can be formalized as follows:

$$\begin{aligned} \underset{e}{\text{argmin}} \quad & f(e) = D(e) = \langle \rho, e \rangle = \rho^T e \\ \text{s.t} \quad & \begin{cases} e \in \{0,1\}^n \text{ binary vector} \\ eH^T = m - xH^T = s \\ e_p \text{ initial solution} \Leftrightarrow e_p H^T = s \end{cases} \end{aligned} \quad (19)$$

with f the objective function and $\rho = \{\rho_i\}_{1 \le i \le n}$ the change cost vector. This is a problem of linear programming written in standard form. It can be solved using the methods simplex or interior points [15].

IV. New Polar Coding Steganographic Algorithm

In [16], we have proposed two approaches for complexity reducing. The first use lookup tables and the second exploits the form of the syndrome but its definition is based on lookup tables. Additionally, only the second approach was implemented in practice. In this section we propose a new version of the second approach which does not need lookup tables, which is implemented in practice and compared to PCS. We will consider constant profile case and wet paper codes.

A. New PCS for Constant Profile

Consider the polar code *PC(4,1)* for the steganography $\mathcal{S}_{PC}(4,3)$. According to (14), the columns $H_{.j}$, $1 \le j \le 4$, of the parity check matrix H satisfy the following equations:

$$\begin{aligned} H_{.1} + H_{.2} &= H_{.3} + H_{.4} = (001)^T \\ H_{.1} + H_{.3} &= H_{.2} + H_{.4} = (010)^T \\ H_{.1} + H_{.4} &= H_{.2} + H_{.3} = (011)^T \end{aligned} \quad (20)$$

When using polar code *PC(8,4)* for steganography $\mathcal{S}_{PC}(8,4)$, the inequalities verified by the columns $H_{.j}$, $1 \le j \le 8$ of the parity check matrix H (15) are:

$$\begin{aligned} &H_{.1} + H_{.2} = H_{.3} + H_{.4} = H_{.5} + H_{.6} = H_{.7} + H_{.8} = (0001)^T \\ &H_{.1} + H_{.3} = H_{.2} + H_{.4} = H_{.5} + H_{.7} = H_{.6} + H_{.8} = (0010)^T \\ &H_{.1} + H_{.4} = H_{.2} + H_{.3} = H_{.5} + H_{.8} = H_{.6} + H_{.7} = (0011)^T \\ &H_{.1} + H_{.5} = H_{.2} + H_{.6} = H_{.3} + H_{.7} = H_{.4} + H_{.8} = (0100)^T \\ &H_{.1} + H_{.6} = H_{.2} + H_{.5} = H_{.3} + H_{.8} = H_{.4} + H_{.7} = (0101)^T \\ &H_{.1} + H_{.7} = H_{.2} + H_{.8} = H_{.3} + H_{.5} = H_{.4} + H_{.6} = (0110)^T \\ &H_{.1} + H_{.8} = H_{.2} + H_{.7} = H_{.3} + H_{.6} = H_{.4} + H_{.5} = (0111)^T \end{aligned} \quad (21)$$

First calculate the syndrome $s = m - xH^T$. If it is equal to:

- **Synd. 1**: zero vector then the embedding change vector e is also equal to zero vector;
- **Synd. 2**: one column of H let be $H_{.j}$ ($s = H_{.j}$), then it has as first element 1 and the embedding change vector e has only one 1 at position j. The columns $H_{.j}$ ($j = 1{:}n$) of H represent the binary values of the numbers between n and $2n$-1 (see, for example, (20) and (21)). Thus, on column j, we have the binary representation of n+j-1. The decimal value $dec(H_{.j}) = n + j - 1$. Hence, $\boldsymbol{j = dec(s) - n + 1}$;
- **Synd. 3**: sum of two columns of H ($H_{.1}$ and $H_{.j}$) then it has a 0 as first coefficient, see (20) and (21). The decimal value varies between 1 and n-1. The embedding change vector has two 1; the first at the first position and the second at

position j. The decimal value of the sum of the two columns $H_{.1}$ and $H_{.j}$ is equal to $((n) + (n+j-1)) \bmod 2n = j-1$. Then $dec(H_{.1}+H_{.j}) = j - 1$. Hence, $\boldsymbol{j = dec(s) + 1}$.

These three cases are also valid for the equivalent[1] systems. According to these observations, there is a relationship between the decimal value of syndrome s and the position of the 1 of the embedding change vector e. A necessary condition is $2^{n-k}=2\cdot n=2^{p+1}$. Then $n-k=p+1$. Hence $k=n-1-\log_2 n=2^p-1-p$. The validity of these observations concerns the values:

$$\begin{aligned} p &\in \{2,3,4,5,6,7\} = \mathcal{P} \\ n &\in \{4,8,\ldots,128\} = \mathcal{N} \\ k &\in \{1,4,\ldots,120\} = \mathcal{K} \end{aligned} \tag{22}$$

with $n = 2^p$, $k = 2^p - 1 - p$ and $p \in \mathcal{P}$.

For an arbitrary polar code $PC(n,k)$ [18], the length n is a power of 2 and the dimension k is a positive integer in {1, 2, …, n-1}. For a polar coding steganographic scheme, the optimality condition [15] is $m = n - k > p = \log_2 n$. The parameters of our polar code in the proposed approach satisfy this optimality condition because we have $n - k = p + 1 > p$.

Consider a given $PC(N=2^P,K)$ for steganography $\mathcal{S}_{PC}(N,N-K)$. If $N \notin \mathcal{N}$ (i.e. $P \in \{8,9,\ldots\} = \mathbb{N} \setminus (\mathcal{P} \cup \{0,1\})$) or $K \notin \mathcal{K}$, we can always come down to a validity case. For $N \in \mathcal{N}$, if $K \in \mathcal{K}$ then we apply directly the steganographic method with $\mathcal{S}_{PC}(N,N-K)$ else we normalize K. For $N \notin \mathcal{N}$, we normalize N and then K.

- **Normalization of *N***: subdivide N in several integers n so that $n \in \mathcal{N}$. Since N and n are both power of 2 ($N = 2^P$ and $n=2^p$), with $N > n$, then N is divisible by any $n \in \mathcal{N}$. The ratio $\frac{N}{n} = \frac{2^P}{2^p} = 2^{P-p} = 2^a$ is a power of 2. Thus, we obtain 2^a segments of size $n \in \mathcal{N}$ each.
- **Normalization of *K***: we aim to bring K back to an integer $k \in \mathcal{K}$. But, since we are interested in the size $m = n-k$ of the message for steganography rather than k, then we will subdivide N-K in $n-k = p+1$ parts such as $n = 2^p \in \mathcal{N}$ and $k = (n-1-\log_2 n) \in \mathcal{K}$. Since we know n, we can determine k. N-K is not always divisible by $n-k$. Let $N-K = (n-k)\cdot q+r$, with $0 \le r < n-k$. If $r = 0$ then we subdivide N-K in q segments of size $n-k$. Otherwise (i.e. $0 < r < n-k$), we have q segments of size $n-k$ and another one of size r. In this case, we complete this segment with $(n-k)-r$ bits 0 to have a size equal to $n-k$.

The embedding is done by pair of a cover medium segment and a message segment. The number of cover segments must be equal to or greater than the number of message segments.

The following algorithm (**Algorithm 1**) calculates a coset leader for a given syndrome s.

Algorithm 1 Calculation of a syndrome coset leader.

Inputs: cover vector x, message m and parity check matrix H.
Outputs: syndrome coset leader e.

1: Initialization:
2: $p \leftarrow$ an element of $\mathcal{P}$; $n=2^p$; $k \leftarrow n-1-p$;
3: e $\leftarrow$ (0, …, 0); y $\leftarrow$ x;
4: Calculation:
5: **If** $xH^T \neq m$ **then**
6: $s \leftarrow m - xH^T$;
7: calculate decimal value of binary syndrome vector
8: (*dec*$\leftarrow$ *decimalConversion* (s))
9: **if** 1st coefficient of syndrome s is equal to 1 **then**
10: affect the *(dec+1-n)-th* coefficient of e to 1;
11: **else**
12: affect 1st and *(dec+1)-th* coefficients of e to 1;
13: **end (if)**
14: **End (If)**

The function *decimalConversion*(s) converts a binary vector s into its decimal value.

For a given parameter p not in validity domain, we can always come down to valid parameter by subdividing it to one of the valid parameters in $\mathcal{P}$. Furthermore, we can choose one of the valid parameters $p \in \mathcal{P}$ and subdivide the cover medium size N to $n \in \mathcal{N}$ and the secret message size to $n-k$ with $k \in \mathcal{K}$. This implies that we can choose the parameter p, which minimizes well the embedding impact.

B. Wet Paper Polar Codes

In this section, we explain how polar codes can be used for the wet paper channel. Give first two theorems that make applicable polar codes for wet paper.

Theorem 1 (Rank of the parity check matrix): The rank of a parity check matrix H of a polar code of block length n and dimension k is

$$\text{rank(H)} = n - k \tag{23}$$

Proof: The generator matrix of the polar code G_n is invertible [18] i.e. the columns of G_n are linearly independents (none of the columns is linear combination of the others). This is equivalent to $\text{rank}(G_n) = n$. The matrix H^T is obtained by pruning the k columns of G_n whose indices are in the information set A [19]. Then G_n is the matrix H^T at which we add k others columns which none is linear combination of the others columns of H^T. Thus $\text{rank}(H^T) + k = \text{rank}(G_n) = n$. Since $\text{rank}(H^T) = \text{rank(H)}$. Then $\text{rank(H)} + k = n$. Finally $\text{rank(H)} = n - k$.

Consider still the set of wet elements $\mathcal{J}$. The maximum number of positions that we can lock for the wet paper steganography is $n - \text{rank(H)} = k$.

Theorem 2 (Maximum number of locked elements): Let $\mathcal{S}_{PC}(n,m=n-k)$ denote the polar coding steganography such that $n \in \mathcal{N}$ and $k \in \mathcal{K}$. The maximum number $\ell_{\max}$ for which we are always able to lock any combination of $\ell_{\max}$ positions is

$$\ell_{max} = \frac{n}{2} - 1 \tag{24}$$

[1] Equivalent denotes the system obtained for another polar coding steganographic parameter n different to 8.

Proof: Consider, for example, the lock of $n/2$ last positions of the cover vector. This amounts to prune the $n/2$ last columns of the parity check matrix H for the matrix product $yH^T = m$. In this case, the second row of the matrix H has all its elements equal to 0 and may then, be written as linear combination of the others (see for example (14) and (15)). This means that we can't always lock $n/2$ positions or more. The maximal number of positions that we can always lock, for any combination, is then less than $n/2$. It is between 1 and $n/2$-1. Let ℓ be the number of locked positions, then $1 \le \ell \le n/2$-1. In our steganographic problem, we must lock a number of positions such that $yH^T = m$ has, at least, one solution. Then, the system must have a number of unknowns more than or equal to the number of equations. The number of unknowns after locking is equal to n-ℓ and the number of equations is n-k = 1+$\log_2(n)$ = 1+p. Thus, we must have n-$\ell \ge n$-k then $\ell \le k$. The value of ℓ have two constrains ($\ell \le n/2$-1 and $\ell \le k$). So ℓ_{max} = min{k, $n/2$-1} = min{n-1-$\log_2(n)$, $n/2$-1}. Prove that ℓ_{max} = $n/2$-1. This amounts to demonstrate that $n/2$-1 ≤ n-1-$\log_2(n)$. That is equivalent to prove that their difference d = n-1-$\log_2(n)$-$n/2$+1 = $n/2$-$\log_2(n)$ = 2^{p-1}-p is positive or null. Consider the following function $f : \mathbb{N} \setminus \{0,1\} \to \mathbb{Z}$ such that $f(p) = 2^{p-1}$-p. This function is continuous and differentiable. Its derivative is $f'(p)=(p-1)\cdot 2^{p-2}$-1 ≥ 0, for $p \ge 2$. This mean that f is monotonic and $f(2) = 0$. Then $f(p) \ge 0$ for any $p \ge 2 \Rightarrow d \ge 0$. Consequently n-1-$\log_2(n) \ge n/2$-1. Finally, we have ℓ_{max} = $n/2$-1.

On the one hand, we can lock k positions but not any ones. On the other hand, any combination of $n/2$-1 positions can be chosen for the locking. Then, to ensure to always succeed the locking, we will not exceed ℓ_{max}.

Let $\mathcal{J}$ be the set of wet elements, then:

- If syndrome s is in **Synd. 1** then we do nothing because e is also a zero vector;
- If s is in **Synd. 2** then consider, by quadruplets, the decimal values of the n syndromes whose embedding change vectors have a single 1. These syndromes correspond to the n columns of H and constitute the half of all possible $2^{n-k} = 2n$. We have $n/4$ quadruplets and each consists of four consecutive syndromes:

$$Q_i = \{n+4i-4;\ n+4i-3;\ n+4i-2;\ n+4i-1\},\ i = 1,\ldots,n/4 \quad (25)$$

Searching to know the quadruplet Q_i of a given syndrome s, we calculate its index i by:

$$i = \lceil (dec(s) - n + 1)/4 \rceil \quad (26)$$

where $\lceil\ \rceil$ denote the ceil operator and dec(s) is the decimal value of the syndrome s.

Proof: According to (25), dec(s) varies between n+4i-4 and n+4i-1 for quadruplet Q_i. Therefore (dec(s)+n+1)/4 is included between i-3/4 and i. Thus, when applying the round to the upper bound then $|(dec(s)+n+1)/4|$ is between $|i-3/4| = i$ and i. This gives (26).

Let s, s_1, s_2 and s_3 be the syndromes forming a quadruplet Q and e, e_1, e_2, e_3 their corresponding embedding change vectors, $e_i \cdot H^T = s_i$, for i=1, 2, 3. In each quadruplet, a syndrome is equal to the sum of the three other; therefore $s = s_1 + s_2 + s_3$. Let $e_4 = e_1 + e_2 + e_3$, then $e_4 \cdot H^T = e_1 \cdot H^T + e_2 \cdot H^T + e_3 \cdot H^T = s_1 + s_2 + s_3 = s$. Thus e_4 is in the coset of s. Consequently, to lock the position j, we choose as embedding change vector e_4. Each of the vectors e_1, e_2, e_3 has only one 1 respectively at different positions j, h, and t. Then e_4 has three 1 at positions h, l and t. If at least one of these three positions is in $\mathcal{J}$, then we search another embedding change vector with 1 at positions not in $\mathcal{J}$. To do so, we choose a pair in the triplet containing one or two elements belonging to $\mathcal{J}$. The chosen pair, let be (h, l), is then replaced by another pair (f, g) which is not included in $\mathcal{J}$ with the equality of an equivalent system of (21) (see **Algorithm 2**). The new embedding change vector will have 1 at positions f, g and t which and 0 at replaced positions h and l.

- If s is in **Synd. 3** (i.e. e has two 1 at positions 1 and j which at least one is in $\mathcal{J}$), then we search with (21) or an equivalent, the pair (h, l) not included in $\mathcal{J}$ using **Algorithm 2**. The embedding change vector will have then two 1 at positions h and l.

For position replacement, the algorithm is as follows:

Algorithm 2 Replacement of a pair by another not in $\mathcal{J}$.

Inputs: pair to replace (i, j) the set of wet element $\mathcal{J}$.
Outputs: the new pair obtained (l, t).

1: **While** (not *found* and not end of $\mathcal{J}$)
2: Search a first position l_1 (from 1 to n) not in $\mathcal{J}$
3: Search a second position t_1 ($t_1 > l_1$) not in $\mathcal{J}$
5: **If** ((l_1, t_1) verifies with (i, j) one of the equalities of (21))
6: $l \leftarrow l_1$; $t \leftarrow t_1$; **return** (l, t);
7: **Else If** (not end of $\mathcal{J}$)
8: Go to line 3.
9: **End (If)**
10: **if** (no good pair (l_1, t_1) is found)
11: Go to line 2.
12: **end (if)**
13: Repeat until having a good pair (l_1, t_1)
14: $l \leftarrow l_1$; $t \leftarrow t_1$; **return** (l, t);
14: **End (While)**

with $bin(a)$ is the binary value of the number a.

The new proposed scheme can be summarized as follows:

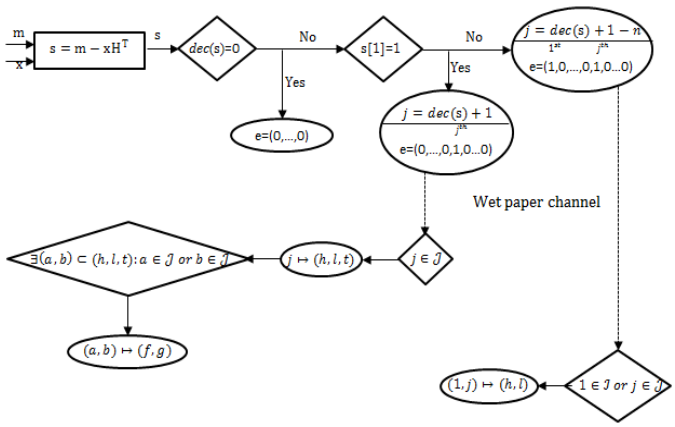


Fig. 4. New polar coding steganographic scheme.

The upper part of the scheme deal with the constant profile case with the three possible cases. In the case of wet paper channel we continuous with the lower side by replacing the wet elements indices. After replacement, the new positions are set to 1 and the old reset to 0 in the embedding change vector e. After calculating e, we can obtain the stego vector by y = x + e.

V. Experimental Results

We have represented in Fig. 5 the embedding efficiency $e=m/D(x,y)$ of the proposed method in wet paper channel according to relative wetness $\tau = |\{i : \rho_i = \infty\}|/n$. We have looked $n/2$-1 elements and then $\tau = (n/2\text{-}1)/n$.

For relative wetness τ varying between 0.25 and 0.5, the embedding efficiency increase from 2.4 to 5.9. The increasing is faster than the relative wetness is great. This proves the goodness of the embedding efficiency.

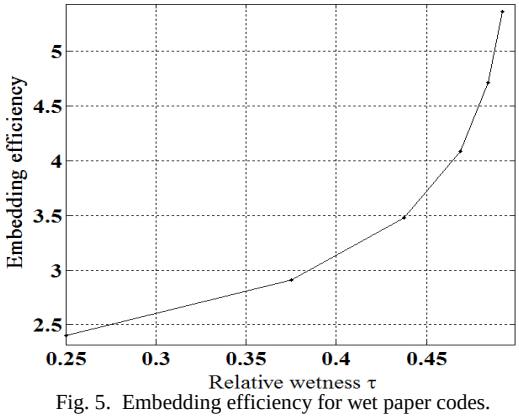


Fig. 5. Embedding efficiency for wet paper codes.

We have also given the complexity variation of the steganographic scheme based on polar codes [15] and those of the algorithm proposed in this paper. To compare the complexity of algorithm PCS with the new algorithm, we measure the required time resources amount for solving the problem of minimizing the embedding impact (here, research of the embedding change vector). For that, we observe their execution time on a computer. We perform several tests on Dual Core CPU running at 3.46 GHz with 2 GB RAM. We chose a polar code of block length $n \in \mathcal{N}$ and dimension $k \in \mathcal{K}$ because our algorithm is applied to these values (see (22)). For each pair $(n,k) \in (\mathcal{N},\mathcal{K})$, 20 cover vectors and 20 messages are randomly generated. Then, we calculate the execution times average (in seconds) of messages embedding in cover vectors. This calculation is done for the two algorithms.

The obtained results for constant profile and wet paper channel cases are respectively represented by Fig. 5 and Fig. 6. Each curve represents specifically the average execution times of the research algorithm of the embedding change vector corresponding to the syndrome calculated from randomly generated cover vector and message. The execution time curve of PCS algorithm is blue and the red one represents the proposed new algorithm.

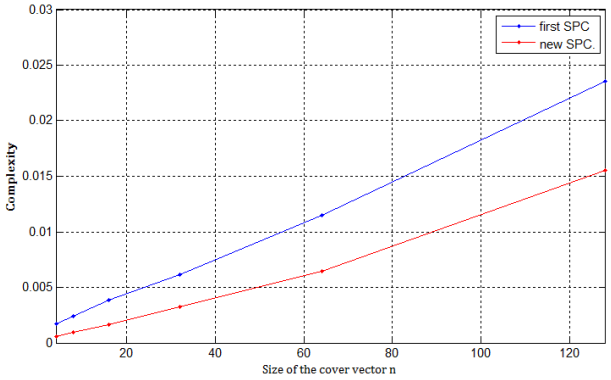


Fig. 6. The execution time of the two schemes for constant profile.

The execution time of the new algorithm is lower than the PCS scheme [15] in constant profile (Fig. 6) as well as in wet paper channel (Fig. 7). The difference between the two curves increases with the size of the cover vector n. This allows us to pronounce on complexity reducing. Therefore, the scheme proposed in this paper allows minimizing the embedding impact with a reduced time complexity when compared to first PCS.

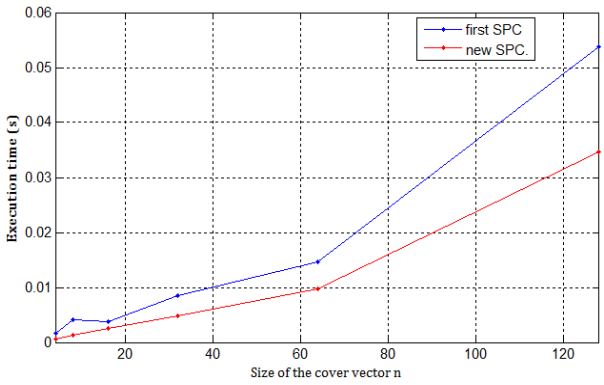


Fig. 7. The execution time of the two schemes for wet paper channel.

We can test the embedding scheme with cover images coming from BOSSbase database version 1.01 (Break Our Stego System) [21] containing 10.000 512×512 8-bit grayscale images of *pgm* format coming from rescaled and cropped natural images of various sizes of eight different cameras.

To make the message less detectable, we choose to permute the pixels of the cover image before embedding. Because the images have a fixed size of 512×512 pixels and 512 is a power of 2, we can use the bit-reversal permutation matrix B_{512}, described in Section II-B, for permutation. This permutation matrix B_{512} can be used to permute the rows and the columns of the cover images before embedding the secret message as shows by Fig. 8. After permutation the obtained image is splitting in $512/n=2^{9-p}$ blocs because the bloc length $n=2^p$ of the used polar code is also a power of 2. Further, we can permute the rows and the columns of these $n \times n$ pixels bloc images using bit-reversal permutation matrix B_n. Then, we repeat the same process as in Fig. 8 with bloc images I^i_{RC} and B_n.

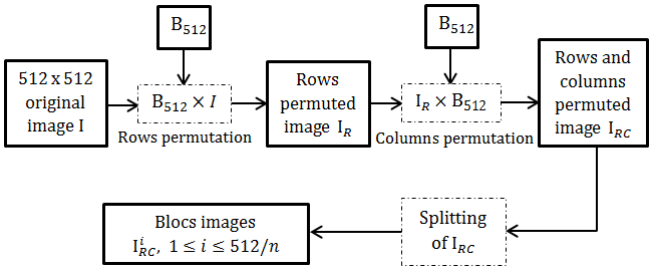


Fig. 8. Permutation and splitting images.

Thus the changes will be scattered over isolated pixels of the image making less detectable the secret message and allowing a more secure insertion. After insertion, it is necessary to find the original order of pixels of the cover image. To achieve this, we still use the matrix B_n since it is invertible and equal to its own inverse. Note that permutation technique was used in the pass but it depended on a key derived from a password. The receiver needed the correct secret key to be able to repeat the permutation which had linear time complexity *O(n)* in [5]. Our permutation technique depends only on the bit-reversal permutation matrix B_n which is already used in the construction of the polar code.

In this manner, we have four images choices to embed the secret message. We can choose the original cover image I, or the rows permuted image I_R, or the columns permuted image I_C, or rows and columns permuted image I_{RC}. This secret choice can be shared with de receiver and is unknown to all another person. The image '28.pgm' of BOSSbase is used to illustrate the permutation effects. The original image and the three permuted images are shows in Fig. 9 (top-left the original image, top-right the rows permuted image, bottom-left the columns permuted image and bottom-right the rows and columns image).

As we can see, the black band on the right columns of the original image is also visible on the rows permuted image. In the same, the white pixels on the top remains on the top rows of the columns permuted image. Conversely, for the rows and columns permuted image the pixels are uniformly distributed.

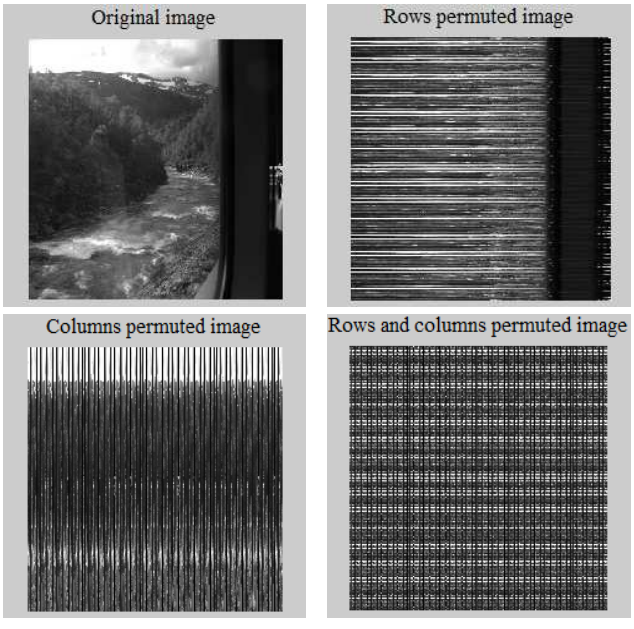


Fig. 9. Original image and different permuted images.

In Fig. 10, white pixels correspond to changes by +1 or −1 and the black ones correspond to pixels that did not change. For the rows and columns permuted image, the changes are uniformly distributed over the whole image (right) when compared to the image without permutation (left) in which the changes are all at the top of the image. The changes in the stego rows and columns permuted matrix will, of course, more hard to be detected by an attacker.

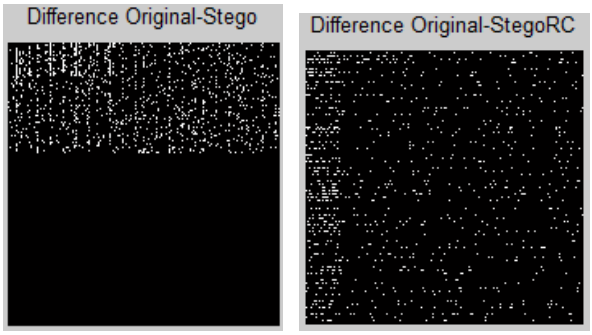


Fig.10. Positions of the embedding changes on non-permuted image (left) and rows and columns permuted image (right) when 0.2 bpp (bit per pixel) is embedded in '28.pgm'.

VI. Conclusion

We proposed, in this paper, new practical steganographic methodology based on polar codes that significantly reduce the complexity of PCS scheme [15] without using lookup tables [16]. This approach exploits the form of the syndrome calculated from the cover medium and the secret message, to determine the embedding change minimizing the distortion function. A relationship between the decimal value of the syndrome and the position of non-zero elements of the embedding change vector is established. This relationship is used to evaluate the changes position on the cover vector. As PCS, this method allows minimizing the embedding impact with a reduced time complexity. The algorithm proposed in this paper provides good performance in terms of embedding efficiency and has a lower time complexity than PCS for both constant profile and wet paper cases as shown by the execution time comparison curves of the two schemes. We have also applied the scheme on images in spatial domain. We have chosen to permute the pixels of images before embedding the private message. The permutation can be done only on the rows or only on the columns or both on the rows and columns of the cover image. This allowed scattering the changes at isolate pixels of the image and made the stego-system more secure.

As part of our future research, we plan to propose an adaptive steganographic scheme based on polar codes using adaptive linear programming decoding of polar codes. We also plan to propose a method of steganalysis.

References

[1] V. Holub, "Content Adaptive Steganography – Design and Detection," *PhD thesis, Binghamton University*, May, 2014.

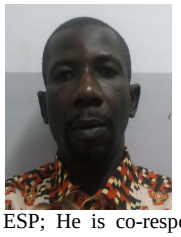
[2] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich and T. Pevný, "Moving Steganography and Steganalysis from laboratory to Real World," In *Proceedings of the ACM IH&MMSec'13, ACM*, pp.ACM 978-1-4503-2081-8/13/06, Montpellier, France, June, 2013.

[3] R. Crandall, "Some notes on steganography," in Steganography *Mailing List* [Online]. Available: http://os.inf.tu-dresden.de/ westfeld/crandall.pdf 1998.

[4] J. Bierbrauer, "On Crandall's Problem," [Online]. Available: http://www.ws.binghamton.edu/fridrich/covcodes.pdf 1998.
[5] A. Westfeld, "High capacity despite better steganalysis (F5 – a steganographic algorithm)," In: *Moskowitz, I.S. (ed.) IH 2001. LNCS*, vol. 2137, pp. 289–302, Springer, Heidelberg, 2001.
[6] M. van Dijk and F. Willems, "Embedding information in grayscale images," in *Proceedings of the 22nd Symposium on Information Communication Theory, Enschede, The Netherlands*, pp. 147–154, May 15–16, 2001.
[7] D. Schönfeld and A. Winkler, "An Embedding with syndrome coding based on BCH codes," in *Proceedings of the 8th ACM Workshop on Multimedia and Security*, pp. 214 – 223, 2006.
[8] R. Zhang, V. Sachnev, H. J. Kim, "Fast BCH syndrome coding for steganography," *S. Katzenbeisser and A.-R. Sadeghi (Eds.), IH 2009, LNCS 5806*, pp. 44-58, Springer-Verlag Berlin Heiderbelg, 2009.
[9] T. Filler and J. Fridrich, "Binary quantization using belief propagation over factor graphs of LDGM codes," presented at the *45th Annual. Allerton Conference Communication, Control and Computing, Allerton, IL*, September, 2007.
[10] W. Zhang and X. Wang, "Generalization of the ZZW embedding construction for steganography," *IEEE Transactions Information Forensics Security*, vol. 4, pp. 564–569, September, 2009.
[11] T. Filler, J. Judas and J. Fridrich, "Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization," *Department of Electrical and Computer Engineering SUNY Binghamton*, USA, 2010.
[12] T. Filler, J. Judas and J. Fridrich, "Minimizing Additive Distortion in steganography Using Syndrome-Trellis Codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, September 2011.
[13] I. Diop, S. M. Farssi, M. Chaumont, O. Khouma, et H. B. Diouf, « Utilisation des codes LDPC en stéganographie, », *COmpression et REprésentation des Signaux Audiovisuels (CORESA)*, pp. 98-104, Lille, France, Mai, 2012.
[14] J. Fridrich, M. Goljan, P. Lisonek and D. Soukal, "Writing on wet paper," *In IEEE Transactions on Signal Processing Third Supplement on Secure Media*, vol. 53, pp. 3923–3935, October, 2005.
[15] B. Diouf, I. Diop, S. M. Farssi, K. Tall, P. A. Fall, A. K. Diop and K. Sylla, "Using of Polar Codes in Steganography," In *Proceedings of the 2nd International Conference on Advances in Computer Science and Engineering (CSE 2013)*, vol. 42, pp. 262-266, Atlantis Press, Los Angeles, July, 2013.
[16] B. Diouf, I. Diop, S. M. Farssi and O. Khouma, "Minimizing Embedding Impact in Steganography Using Polar Codes," In *Proceedings of 4rd IEEE International Conference on Multimedia Computing and Systems (ICMCS'14)*, pp. 105–111, Marrakesh, Morocco, April, 2014.
[17] B. Diouf, I. Diop, S. M. Farssi and O. Khouma, "Practical Polar Coding Method to Minimize the Embedding Impact in Steganography," In *Proceedings of the IEEE International Science and Information (SAI) Conference*, London, United Kingdom, July, 2015.
[18] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions Information Theory*, vol. IT-55, pp. 3051-3073, July, 2009.
[19] N. Goela, S. B. Korada, and M. Gastpar, "On LP Decoding of Polar Codes," *Submitted to IEEE Transaction Information Theory Workshop-ITW*, Dublin, 2010.
[20] T. Pevnỳ, T. Filler and P. Bas, "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography," *Czech Technical University, Prague, Czech Republic; State University, New York in Binghamton, NY, USA; CNRS-LAGIS, Lille, France*, 2010.
[21] T. Filler, T. Pevný, and P. Bas. BOSS (Break Our Steganography System). http://www.agents.cz/boss, July 2010.
[22] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX (E. J. Delp and P. W. Wong, eds.)*, vol. 6505, pp. 02–03, San Jose, CA, January 29–February 1, 2007.
[23] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *Proceedings 8th International Workshop Information Hiding, J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, Eds., Alexandria, VA*, vol. 4437, Lecture Notes in Computer Science, pp. 314–327, July 10–12, 2006.

Birahime Diouf received the Electronic and Telecommunications Engineering Degree from Gaston Berger University (UGB), Saint-Louis, Senegal in 2012, and the M.Sc. in Computer Science, Modeling and Simulation of Complex Systems from Polytechnic Institute, Cheikh Anta Diop University (UCAD), Dakar, Senegal in 2013. He is currently working towards the Ph.D. degree.

He is currently a Researcher at the Department of Computer Science, Polytechnic Institute, Cheikh Anta Diop University. His research interests include data hiding, information theory, coding theory, image processing and signal processing.



Idy DIOP graduated from the University of Dakar. He received his engineering degree from Electronic and telecommunication in 2006 to the Gaston Berger University of Saint-Louis of Senegal, and a Diploma of master research: Physics for Engineers in Ecole Supérieure Polytechnique (ESP), Dakar-Senegal (2007). He holds a PhD in Engineering Thesis (2011): watermarking medical image based on JPEG 2000 ESP; He is co-responsible of several memories of Master in Computer Science and Telecommunications, author of several publications in international journals and several studies reported with publications in the proceedings of International Congresses with peer and scientific committee member of several international conferences. His research interests include steganography, steganalysis, compression, watermarking, information and coding theory and wireless communications.

Sidi Mohammed FARSSI graduated from the University of Dakar. He received his engineering degree from Electrical Engineering Design option (EEAI) in 1988 to the ESP, and a Diploma of Advanced Studies: Physics for Engineers in Paris XII (1989). He holds a PhD in Engineering Thesis (1993): Biomedical image processing in ESP (Ecole Supérieure Polytechnique de Dakar- Senegal) and then PhD State es-sciences (1997): Biomedical Image Processing, Dakar ESP. He is Director of several doctoral theses in Information Processing, Director of several DEA in Computer Science and Telecommunications, Director of several memories of Master in Computer Science and Telecommunications, author of several publications in international journals and several studies reported with publications in the proceedings of International Congresses with peer, expert player in international scientific journals, scientific committee member of several international conferences, participating in several workshops and training expertise, expert for the United Nations University for Education and Scientific Research, Member of the reflection of TOKTEN project, Expert of 'World ORT Union, Member of Networks of Excellence SIMILAR, Member of the Society of African scientists, Expert for the recognition and equivalence of degrees to African schools CAM, Expert for the Association of Francophone universities AUF..

Volume. 5 Issue. 5