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

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 1 Issue 1, Jul 2012, ISSN: 2288-0003

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

Global IT
Research Institute

Journal Editorial Board

Editor-in-Chief

Editors

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 1, Issue 1

Joint Source-Channel Coding with Unequal Error Protection using Asymmetric Turbo Codes

Hanxin WANG, Cuitao ZHU, Chengyi XIONG and Shaoping CHEN

Department of Electronics and Information Engineering, South-Central University for Nationalities, Wuhan, China

wanghx8888@163.com, zhucuitao@163.com, xiongchengyi@qq.com, spchen@scuec.edu.cn

***Abstract*—In this paper, we devise an efficient joint source-channel coding scheme for robust image transmission over noisy channels. We firstly present a novel interleaver, named unequal row column cyclic cross interleaver, which could improve the error correction capability of turbo codes effectively. Secondly, we devise two types of asymmetric turbo codes which consist of the parallel concatenated turbo codes using two non-identical component encoders with the different constraint lengths and mixed types of generator polynomials. The presented asymmetric turbo codes can optimize the bit error rate of both water-fall region at low signal to noise ratio and error-floor region at high signal to noise ratio, they outperform the conventional symmetric turbo codes but with reduced decoding complexity. Finally, we propose a joint source-channel coding scheme based on unequal error protection using asymmetric turbo codes. This scheme can adaptively adopt different coding strategies, different interleavers of turbo codes, various decoding algorithms and appropriate decoding iterative numbers according to the different significant levels of image data streams and the varying conditions of estimated channel state information. The proposed scheme can also dynamically adjust the source compression ratios and channel code rates by optimizing the rate allocation according to the calculated peak signal to noise ratio of reconstructed images and the estimated channel states information. The experimental results show that the proposed joint source-channel coding scheme can evidently increase the peak signal to noise ratio of the reconstructed images and improve the visual effect of the images but with no additional bandwidth, the scheme is more adaptive and feasible.**

***Index Terms*—Joint source-channel coding; Unequal error protection; Asymmetric turbo codes; Interleaver; Bit error rate; Water-fall, Error-floor; Peak signal to noise ratio**

I. INTRODUCTION

With the development of wireless multimedia communication services, the fast growing consumer demand has spurred more interest in the image and video data transmission over noisy channels. The varying wireless channel causes high transmission errors for multimedia data streams and results in deterioration of reconstructed image and video qualities. To enhance the efficiency and reliability of data streams, source data compression and channel errors correction technologies are two effective solutions in the digital multimedia communication. On the one hand, the source data have numerous redundant information which require to be processed. Compressed data streams are very sensitive to channel errors because their most redundancy bits are removed. Sometimes a few errors may destroy the entire data streams and thus affect the qualities of restored image and video. On the other hand, a large amount of channel errors could occur due to the poor wireless channels whose capacities are limited and time-varying. Considering the characteristics of both source data streams and channel state information (CSI), joint source-channel coding (JSCC) is a promising approach to achieve better performance in limited bandwidth and limited power system. JSCC technique has been attractive in delay-sensitive multimedia transmission system, especially in heterogenous networks where users may have different quality of service (QoS) requirements [1] [2]. JSCC has two main design issues. One is to design an appropriate channel protection method, and the other is to optimally allocate the given bandwidth resource between the source code and the channel code so as to achieve the best possible end-to-end performance in the noisy environment [3]. Unequal error protection (UEP) is an intelligent solution for JSCC. UEP is often applied to Forward Error Correction (FEC), the data bits are grouped according to some criteria capable of determining their importance to the restored source data, and the different channel codes are assigned to different source bit groups [4] [5] [6]. In recognition of the fact that the effects of bit errors in encoded sources are usually more detrimental in some bit groups than in others, several UEP schemes for image transmission using turbo codes are reported according to the significant levels of the image bit streams and varying channel characteristic [7], [8], [9]. But most of them mainly focus on UEP with conventional symmetric turbo codes (STC). However, STC evidently exist some defects that

Manuscript received May 3, 2012. This work was sponsored by the National Natural Science Foundation of China with Grant No.60972081, No.61072075, the Natural Science Foundation of State Ethnic Affairs Commission with Grant No.10ZN07 and the Key Project for the Natural Science Foundation of Hubei Province with Grant No.2009CDA139, it was also supported by International Fellowship Researcher of Chonbuk National University of Korea with Grant No. IFR2002.

Hanxin WANG is with the Department of Electronics and Information Engineering, South-Central University for Nationalities, Wuhan, China (Tel: 86-13343589736; fax: 86-027-67842815; email: wanghx8888@163.com)

Cuitao ZHU is with the Department of Electronics and Information Engineering, South-Central University for Nationalities, Wuhan, China (email: zhucuitao@163.com)

Chengyi XIONG is with the Department of Electronics and Information Engineering, South-Central University for Nationalities, Wuhan, China (email: xiongchengyi@qq.com)

Shaoping CHEN is with the Department of Electronics and Information Engineering, South-Central University for Nationalities, Wuhan, China (email: spchen@scuec.edu.cn)

they have either a good water-fall performance at low signal to noise ratio (SNR) or a good error-floor at high SNR, but not both over the entire range of SNR [10]. Asymmetric Turbo codes (ATC) are the better choice among the improvement of performance, the overall time delay and the computational complexity of decoding algorithms. Several ATC are investigated to improve bit error rate (BER) in the whole SNR ranges compared with STC [11], [12]. This paper presents an effective JSCC design based on UEP using ATC, which can adaptively adopt different coding strategies, different interleavers of turbo codes, various decoding algorithms and appropriate decoding iterative numbers in terms of the different significant levels of source bit streams and the varying conditions of estimated CSI. This scheme can dynamically adjust the source compression ratios (CR) and channel code rates according to the calculated peak signal to noise ratio (PSNR) of the reconstructed images and the estimated channel conditions. The proposed scheme can also evidently increase PSNR of the images and improve the visual effect of the images but with no additional bandwidth. The remainder of paper is organized as follows. In section II, we present a novel interleaver named unequal row column cyclic cross (URCCC) interleaver, it could improve the error correction capability of turbo codes effectively. In section III, we devise two types of ATC using the different constraint lengths and mixed types of generator polynomials to optimize the BER performance of both water-fall and error-floor for turbo codes. In Section IV, focusing on the characteristic that the image data streams compressed by set partitioning in hierarchical trees (SPIHT) algorithm have different sensitivity to channel bit errors, we propose an efficient JSCC scheme with UEP using the designed ATC. The simulation results for JSCC are shown in section V and the conclusions are drawn in the last section.

II. UNEQUAL ROW COLUMN CYCLIC CROSS INTERLEAVER

The interleaver is one of the essential components for turbo codes and plays an important role in determining the performance and decoding computational complexity, because the interleaver directly affects the distance properties of the turbo codes. An interleaver is used between the two constituent encoders of turbo codes to provide randomness and produce high weight codewords. The design aim of a good code-matched interleaver is to eliminate low weight codewords with significant contributions to the error performance and to reduce the number of other low weight codewords which could not be eliminated [13], [14], [15]. Considering the drawbacks of common block and random interleavers which can not eliminate the more information bits correlation or not permute the low weight codewords sequence effectively, we present a new unequal row column cyclic cross interleaver, i.e. URCCC. This new interleaver can more thoroughly eliminate the information bits correlation than block and random interleavers, it can also permute the low weight codewords sequence into high weight codewords ones.

A. Algorithm of URCCC interleaver

To improve the BER performance of turbo codes significantly, the good interleaver can be implemented to avoid low weight codewords and to provide sufficient randomness for the input sequences. Many interleavers have been done on design of turbo codes. The block and random interleavers are the most commonly used in turbo codes. But they can not preferably produce the fewest output codewords sequence with low weight. An optimal interleaver should be able to generate the largest minimum codewords weight with the lowest number of codewords of that weight. So, a novel interleaver, named URCCC, is firstly proposed to offer superior performance for ATC design. The proposed algorithm of URCCC is described as follows:

Step 1: Information bits data are written into $m \times n$ block interleaver matrix in row wise from left to right and top to bottom, as shown in Figure 1 (a). For convenience of description, we set $m = 8$ and $n = 8$, the data in Figure 1 represents bits sequence number of information data.

Step 2: Odd row bits data are rearranged as follow formula (1) and even row data are reordered as formula (2), respectively. C_i denotes interleaver table, i is column number, n is column length, mod denotes modular arithmetic, k and p are adjustable parameters, $k < n$, $p < n$, k and p are relatively prime to n, while $k \neq p$. The process result is shown in Figure 1 (b).

$$C_i = (k \times i)(\mathrm{mod}\, n) + 1, \qquad 0 < i \le n \tag{1}$$

$$C_i = (p \times i)(\mathrm{mod}\, n) + 1, \qquad 0 < i \le n \tag{2}$$

Step 3: Odd column bits data are rearranged as follow formula (3) and even column bits data are reordered as follow formula (4), respectively. C_j is also interleaver table, j is row number, m is row length, a and b are adjustable parameters, $a < m$, $b < m$, a and b are relatively prime to m, while $a \neq b$. The process result is shown in Figure 1 (c).

$$C_j = (a \times j)(\mathrm{mod}\, m) + 1, \qquad 0 < j \le m \tag{3}$$

$$C_j = (b \times j)(\mathrm{mod}\, m) + 1, \qquad 0 < j \le m \tag{4}$$

Step 4: The interleaved bits data are read out from interleaver matrix of Figure 1 (c) in column wise from top to bottom and left to right.

The good interleaver design would be capable of providing sufficient randomness. For some special information bit streams, such as low weight and symmetric bit data, the different interleavers can obtain complete different interleaved effectivenss. E.g. the input bits sequence 100000010... 010000001, the output bits data sequence after the block interleaver are all the same as the original input sequence, as shown in figure 2 (a), it can't reach the purpose of interleaver. But using URCCC interleaver, the input sequence is well permuted randomly, it can avoid the appearance of the fixed point, as shown in figure 2 (b). Here, the data in Figure 2 represents information bits.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig. 1 (a)

4	7	2	5	8	3	6	1
14	11	16	13	10	15	12	9
20	23	18	21	24	19	22	17
30	27	32	29	26	31	28	25
36	39	34	37	40	35	38	33
46	43	48	45	42	47	44	41
52	55	50	53	56	51	54	49
62	59	64	61	58	63	60	57

Fig. 1 (b)

30	43	32	45	26	47	28	41
52	23	50	21	56	19	54	17
14	59	16	61	10	63	12	57
36	39	34	37	40	35	38	33
62	11	64	13	58	15	60	9
20	55	18	53	24	51	22	49
46	27	48	29	42	31	44	25
4	7	2	5	8	3	6	1

Fig. 1 (c)

Fig. 1. Design for URCCC interleaver
(a) step 1 (b) step 2 (c) step 3

1	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1

Fig. 2 (a)

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	1

Fig. 2 (b)

Fig. 2. Effectivenss of the different interleaver
(a) Block interleaver (b) URCCC interleaver

B. Simulation and Analysis of URCCC interleaver

The BER performance simulations of URCCC interleaver used in turbo codes is shown in Figure 3. For the ease of comparison, the simulation results of block and random interleavers are also drawn. In simulation experiments, information bits size is 378, generator polynomials of two component codes for turbo codes are 13 and 15 (in octal), one half code rate, 4 iteration number for log-MAP algorithm, BPSK modulation, AWGN channel. It is observed that URCCC interleaver outperform conventional block and random interleavers.

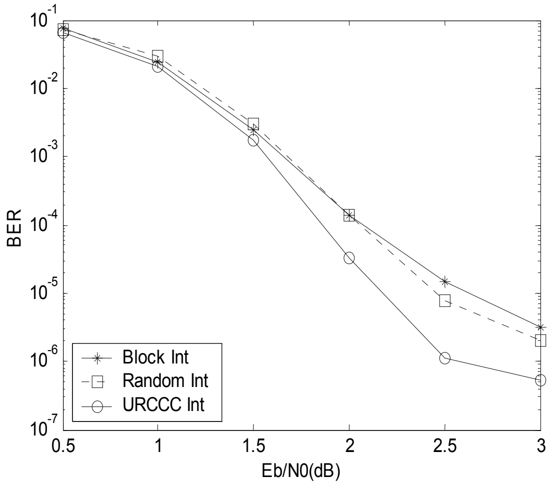


Fig. 3. BER versus E_b/N_0 for URCCC interleaver in turbo codes

URCCC interleaver can not only reduce the more information sequence correlation than block and random interleavers, it can also permute the low weight codewords sequence into high weight codewords sequence and significantly improve the performance of turbo codes. In the whole process of interleaving algorithm, URCCC interleaver are based on linear modular arithmetic, it has faster calculation speed and low complexity hardware requirement. For the process of row or column interleaving, it would complete only through the simple cyclic operation but not with a interleaving memory table, so it can save storage space. Moreover, URCCC interleaver has adjustable parameters, it can dynamically select the parameters to adapt for various channel states and to improve the system error correction capability, the presented URCCC interleaver is more flexibility and robust.

III. ASYMMETRIC TURBO CODES

A. Review of Turbo Codes

Turbo codes have a near Shannon limit error correction capability through iterative decoding based on soft-input and soft-output (SISO) decoding algorithm. Turbo codes have been widely used in the wireless mobile communication system [16]. The conventional STC consist of two parallel concatenated recursive systematic convolutional (RSC) constituent encoders separated by an interleaver. Generally, these constituent encoders are the identical component codes with the same constraint lengths and the same generator polynomials [17], [18]. The BER performance curve of turbo codes is divided into two regions. The first region is called water-fall in lower SNR, the BER curve decreases rapidly at water-fall region. The second region is error-floor in higher SNR, the curve flattens in this region [10]. The STC have either good water-fall performance in lower SNR or good error-floor in higher SNR, but not both over the entire ranges of SNR. ATC are the better trade-off among the improvement of performance, overall delay and computational complexity of decoding algorithm. The performance evaluation of the ATC for the 3rd generation communication system (3G) are given in [11], [12].

ATC encoder is composed of two different parallel concatenated RSC1 and RSC2 encoder separated by an interleaver (Int), as shown in Figure 4. u_k is input information bit streams, x_k^s is the systematic information bits, x_k^{1p} and x_k^{2p} are the parity bits generated by RSC1 and RSC2, respectively. Puncturing of parity bits x_k^{1p} and x_k^{2p} can achieve the various required code rate. c_k is the coded bit streams which are consisted of x_k^s and x_k^p by parallel-to-serial (P/S) multiplexer.

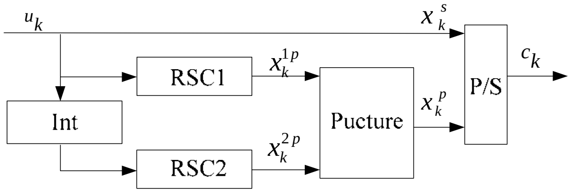


Fig. 4. ATC encoder

The coded bits c_k are then binary phase shift keying (BPSK) modulated and transmitted through an additive white Gaussian noise (AWGN) channel with a double sided power spectral density of *N₀ /2*. At the receiver, the matched filter output y_k is multiplied by the channel reliability value L_c, as shown in Figure 5, $L_c = 4 \cdot (E_b / N_0) \cdot R$, where E_b / N_0 denotes received bit energy to noise power ratio and R represents the code rate [16]. Through serial-to-parallel (S/P) de-multiplexer, $L_c y_k$ is separated into $L_c y_k^s$, $L_c y_k^{1p}$ and $L_c y_k^{2p}$ corresponding to the systematic and two parity bits, respectively.

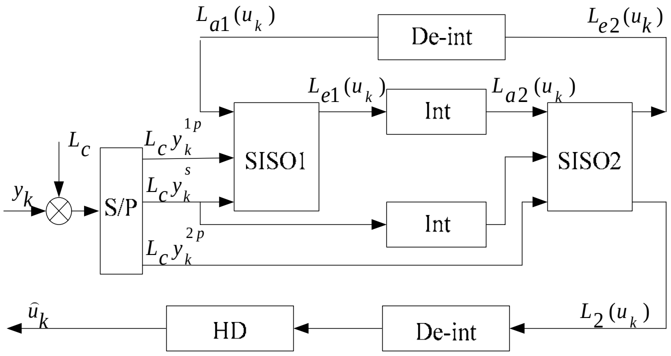


Fig. 5. ATC decoder

At the first iteration of decoding, a priori Log Likelihood Ratio (LLR) value of SISO1 decoder $L_{a1}(u_k)$ is initially set to 0, the systematic bits LLR value $L_c y_k^s$ and parity bits LLR value $L_c y_k^{1p}$ are inputted into SISO1 decoder. The extrinsic LLR value $L_{e1}(u_k)$ produced by SISO1 decoder is interleaved and sent to SISO2 decoder as a priori value $L_{a2}(u_k)$. Moreover, $L_c y_k^{2p}$ and interleaved $L_c y_k^s$ are simultaneously sent to SISO2 decoder to produce extrinsic value $L_{e2}(u_k)$, and then $L_{e2}(u_k)$ is de-interleaved (De-int) and fed back to SISO1 decoder as a priori value for the next decoding iteration. The iterative decoding will keep on working until either a stopping criteria is met or a preset maximum number of iterations is reached. When the iterative decoding is finished, the output value $L_2(u_k)$ of SISO2 decoder is de-interleaved and sent to hard decision (HD) to produce estimated value $\hat{u}_k$.

B. Proposed Two Types of ATC

Compared with STC, the constraint lengths or generator polynomials of two RSC component codes are different for ATC. Here, we design two types of ATC which consist of the parallel concatenated turbo codes using the non-identical RSC component codes with the different constraint lengths or the different types of generator polynomials.

1) Type-I of ATC:

Type-I of ATC consist of two different component codes with the identical constraint lengths but the different types of generator polynomials. As we all know, the performance of turbo codes at low SNR is determined by the distance spectrum, but the performance at high SNR is determined by the effective free distance. There are a number of key design parameters involved in determining the distance spectrum and free distance for turbo codes, such as the choice of component encoders and the types of interleavers, etc. Several interleavers are designed to improve BER performance of turbo codes [13], [14], [15]. Here, we firstly focus all attention on using the different component codes with the primitive and non-primitive feedback generator polynomials to construct ATC, because the component codes with non-primitive generator polynomials may optimize the distance spectrum to improve water-fall performance and primitive generator polynomials may enlarge the free distance to reduce error-floor.

For convenience, the generator polynomial is denoted by G (in octal), the constraint length is denoted by K, respectively. P-G denotes primitive generator polynomial of the constituent encoder of turbo codes, NP-G denotes non-primitive polynomial. The various generator polynomials with constraint lengths K=3, 4, 5 and the types of the primitive and non-primitive polynomials are listed in Table I.

TABLE I
The various constraint lengths and the types of generator polynomials

Constraint lengths	**Generator polynomials**	
	P-G	**NP-G**
K=3	G=[7, 5]	G=[5, 5]
K=4	G=[13,17]	G=[15,17]
K=5	G=[23,35]	G=[37,21]

And then, four type-I of ATC with the same constraint lengths but mixed types of generator polynomials are presented, as shown in Table II. Here, K1 and K2 denote constraint lengths of two component codes RSC1 and RSC2, respectively ； G1 and G2 denote generator polynomials of RSC1 and RSC2, P and NP denote primitive and non-primitive polynomial, suffix 1, 2 of P and NP are corresponding to RSC1 and RSC2. We select K1=K2=5. In fact, P1-P2 and NP1-NP2 turbo codes with the same constraint lengths are just the conventional STC.

TABLE II
Type-I of ATC with the same constraint lengths and mixed types of generator polynomials

Constraint lengths	**Generator polynomials**			
	P1-P2	**NP1-NP2**	**NP1-P2**	**P1-NP2**
K1=5	G1=[23,35]	G1=[37,21]	G1=[37,21]	G1=[23,35]
K2=5	G2=[23,35]	G2=[37,21]	G2=[23,35]	G2=[37,21]

2) Type-II of ATC:

Type-II of ATC consist of two non-identical component codes with the different constraint lengths and mixed types of generator polynomials. On the one hand, the constraint length of the constituent encoder for turbo codes plays an important role in determining the performance and decoding computational complexity. Free distance is shorter for turbo codes with shorter constraint length, it can cause poorer error-floor performance. Turbo codes with longer constraint length can achieve longer free distance and better performance, but the computational complexity will increase correspondingly. In order to obtain good performance and reduce decoding computational complexity, it is necessary to decrease the constraint lengths of one constituent encoder of STC. And then, type-II of ATC can be constructed by using two component codes with different constraint lengths. On the other hand, the types of generator polynomials of component encoder are a key factor for ATC design. The primitive feedback generator polynomials for component code are known to be able to enlarge the free distance to improve error floor at high SNR, but at a cost of degrading water-fall at low SNR. On the contrary, the non-primitive generator polynomials would optimize the distance spectrum to enhance water-fall performance at low SNR, but reduce error-floor at high SNR. For this reason, type-II of ATC can also be constructed by using two component codes with mixed types of the primitive and non-primitive generator polynomials.

The constraint length K=5 of one of the constituent encoders of conventional STC in [17] is reduced to 3 and 4, primitive and non-primitive polynomial are chosen as feedback generator polynomials of two constituent codes. According to Table 1, Our proposed sixteen types-II of ATC with the different constraint lengths and mixed types of the generator polynomials are listed in Table III.

TABLE III
Types-II of ATC with different constraint lengths and mixed types of generator polynomials

Constraint lengths	**Generator polynomials**			
	P1-P2	**NP1-NP2**	**NP1-P2**	**P1-NP2**

K1=3
K2=5
	G1=[7, 5]
	G2=[23,35]
		G1=[5, 5]
		G2=[37,21]
			G1=[5, 5]
			G2=[23,35]
				G1=[7, 5]
				G2=[37,21]

K1=5
K2=3
	G1=[23,35]
	G2=[7, 5]
		G1=[37,21]
		G2=[5, 5]
			G1=[37,21]
			G2=[7, 5]
				G1=[23,35]
				G2=[5, 5]

K1=4
K2=5
	G1=[13,17]
	G2=[23,35]
		G1=[15,17]
		G2=[37,21]
			G1=[15,17]
			G2=[23,35]
				G1=[13,17]
				G2=[37,21]

K1=5
K2=4
	G1=[23,35]
	G2=[13,17]
		G1=[37,21]
		G2=[15,17]
			G1=[37,21]
			G2=[13,17]
				G1=[23,35]
				G2=[15,17]

C. Simulation and Analysis of ATC

For all simulations of two types of ATC, the information size is set to 378 bits, the constraint lengths K are 3, 4 and 5, maximum number of iteration is 8, one-half code rate, URCCC interleaver, SISO decoder, log-MAP decoding algorithm, BPSK modulation, AWGN channel.

Figure 6 gives the BER versus E_b/N_0 for the type-I of ATC with the same constraint lengths and mixed types of generator polynomials. Here, we take K1=K2=5. It was observed from the simulation results in Figure 6:

(1) The error-floor performance of P1-P2-STC is good at high SNR, but its water-fall is poor at low SNR. On the contrary, the water-fall of NP1-NP2-STC is superior at low SNR, but its error-floor is inferior at high SNR.

(2) At low SNR, the water-fall of NP1-P2-ATC and P1-NP2-ATC is superior to P1-P2-STC but inferior to NP1-NP2-STC. However, the error-floor of NP1-P2-ATC and P1-NP2-ATC is inferior to P1-P2-STC but superior to NP1-NP2-STC at high SNR.

These simulation results effectively indicate that the type-I of ATC is optimal trade-off scheme over the entire range of SNR.

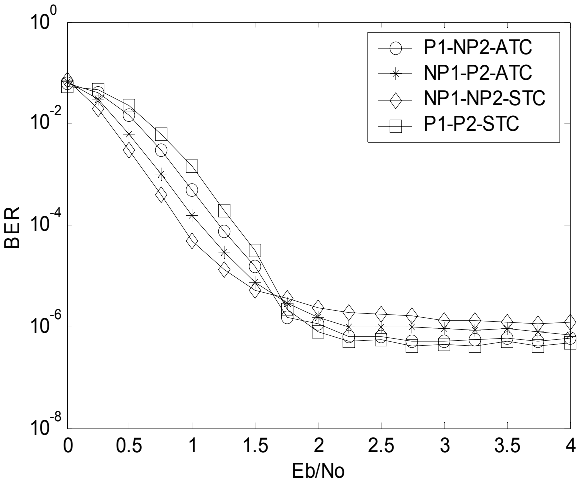


Fig. 6. BER versus E_b/N_0 for type-I of ATC with the same constraint lengths K1=K2=5 and mixed types of generator polynomials

Figure 7 shows the BER versus E_b/N_0 for the type-II of P1-P2-ATC with the different combination of the constraint lengths K=3, 4, 5 and the same primitive generator polynomials. For the ease of comparison, the BER versus E_b/N_0 for the P1-P2-STC with K1=K2=5 and primitive generator polynomials is also shown in Figure 7, the simulation analysis and conclusions are as follow:

(1) By decreasing the constraint lengths of one constituent encoder of STC, the water-fall and error-floor performances of type-II of ATC are all become deteriorated. It is caused by the smaller free distance of the component codes with short constraint lengths. However, the computational complexity of decoding algorithm can be reduced for the type-II of ATC with short constraint lengths. It is demonstrated that type-II of ATC can get a favorable trade-off between the performance and computational complexity.

(2) The performance of ATC with K1=4, K2=5 or K1=5, K2=4 is slightly inferior to STC with K1=K2=5. Especially, the performance of ATC with K1=5, K2=4 is nearly close to conventional turbo codes with negligible performance degradation but with a reduced computational complexity.

(3) The ATC with K1=5, K2=4 is superior to one with K1=4, K2=5. Similarly, the ATC with K1=5, K2=3 is superior to that with K1=3, K2=5. It is evident that reducing the constraint length of RSC2 component code is a good scheme when this type-II of ATC with the different constraint lengths are constructed.

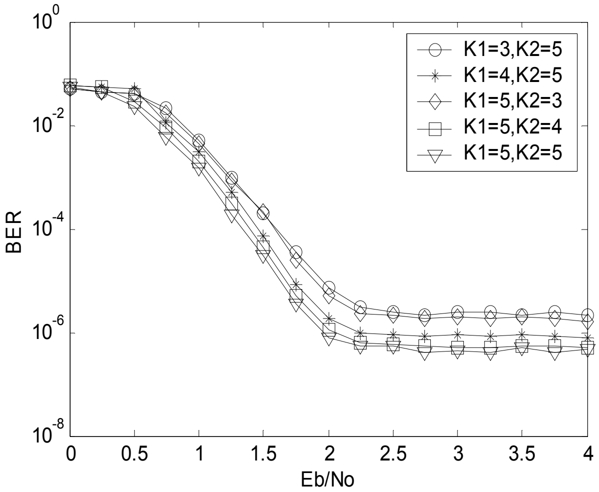


Fig. 7. BER versus E_b/N_0 for type-II of P1-P2-ATC with the different constraint lengths and the same primitive generator polynomials

The BER versus E_b/N_0 for the type-II of ATC with the different constraint lengths and mixed types of generator polynomials is shown in Figure 8. Here, we select K1=5, K2=4.

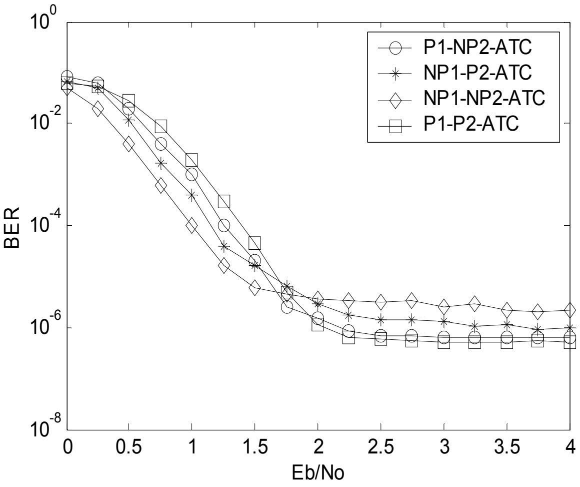


Fig. 8. BER versus E_b/N_0 for ATC with the different constraint lengths and mixed types of generator polynomials

Our analysis and conclusions from figure 8 are as follow:

(1) At low SNR ($E_b/N_0 \leq$ 1.75dB), the performance of NP1-NP2-ATC is the best, NP1-P2-ATC better, P1-NP2-ATC inferior, P1-P2-ATC poor. But at high SNR ($E_b/N_0 \geq$ 1.75dB), the results are in reverse order. The reason is that the non-primitive generator polynomials can optimize the distance spectrum to improve water-fall performance of turbo codes and the primitive polynomials enlarge the free distance to reduce error-floor.

(2) Considering the entire range of SNR ($0\text{dB} \le E_b/N_0 \le 4\text{dB}$), NP1-P2-ATC and P1-NP2-ATC are the better trade-off between the water-fall and the error-floor performance. Evidently, NP1-P2-ATC and P1-NP2-ATC are superior to P1-P2-ATC and NP1-NP2-ATC turbo codes over the entire range of SNR.

Therefore, it is a good choice that one constituent encoder is commonly constructed by using a primitive generator polynomial and another using non-primitive polynomial when this type-II of ATC are designed.

IV. JOINT SOURCE-CHANNEL CODING WITH UEP USING ATC

A. UEP Scheme using ATC

In digital multimedia communication system, the sensitivity of the image or video bit streams to channel errors is generally not uniform, the reconstructed image or video is insensitive to errors affected by insignificant bit streams (e.g. high frequency components of image), while it is rather sensitive to errors caused by significant bits (e.g. low frequency components of image), i.e. the sensitivity of the significant bits to errors is far greater than the insignificant bits. E.g. eight bits quantized gray-scale image, the priority of eight bits for per pixel is different, the sensitivity of the Most Significant Bits (MSB) to errors is greater than the Least Significant Bits (LSB). Here, we propose an UEP scheme for image transmission by using the ATC. We classify source data into several classes and use UEP encoder to strongly protect the important classes bit streams and weakly protect the non-important classes. The diagram of UEP encoder is shown in Figure 9.

According to the different importance levels, image data streams are divided into three blocks and then hierarchically coded by UEP encoder. Specific processes are as follows:

(1) Image bit streams X are partitioned into three groups so that the important bits can obtain strong protection. The first group consists of three MSB bits for per pixel, it is so called most significant bit streams X1. The second group is composed by two middle bits, named significant bit streams X2. The third group is comprised of three LSB bits, denoted as insignificant bit streams X3.

(2) In terms of different importance classes of image bit streams, the UEP encoder adaptively adopts different types of turbo codes. For X1, ATC or STC with constraint lengths K1=5 and K2=5 are chosen because they have the best performance to protect X1 strongly. For X2, ATC with constraint lengths K1=5 and K2=3 are selected due to their relative low complexity and moderate error correction ability. For X3, ATC or STC with constraint lengths K1=3 and K2=3 are chosen because of their most low complexity and lower time delay.

(3) On the conditions of CSI from channel estimator, the UEP encoder adaptively adjusts coding strategies through the switch S1, S2, S3. If the CSI is good, i.e. high SNR, then the encoder chooses P1-P2-STC or P1-P2-ATC because of their best error-floor performance. If the CSI is slightly inferior, i.e. medium SNR, then chooses NP1-P2-ATC or P1-NP2-ATC because of their best trade-off between water-fall and error-floor performance. If the CSI is worse, i.e. low SNR, then chooses NP1-NP2-STC because of their best water-fall performance.

The presented UEP scheme both considers conditions of CSI from channel estimator and the bits error effect of the different importance levels of image bit streams, it can achieve the better trade-off among the reliability, the time delay and the computational complexity.

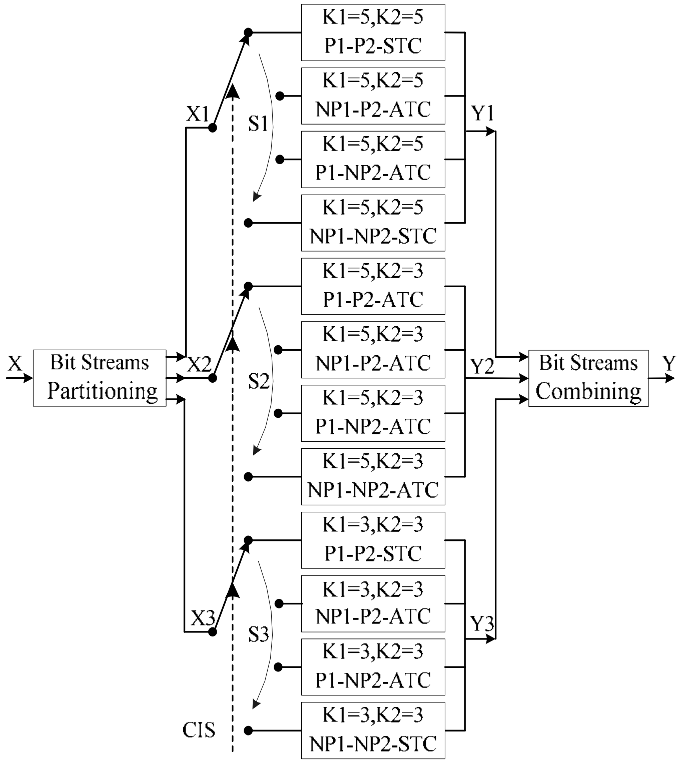


Fig. 9. UEP encoder using ATC

B. JSCC with UEP using ATC

With above mentioned UEP design using ATC, we present an effective JSCC scheme. The block diagram of the JSCC is shown in Figure 10.

Original image is firstly decomposed by discrete wavelet transformation (DWT) and compressed by SPIHT encoder [19] [20] [21]. As the importance levels of the compressed bit streams X trend towards decreasing progressively, i.e. the significant bit streams locate the nearer front and the insignificant bit streams are behind, we would partition X into three classes block, X1, X2 and X3. Then they are encoded with UEP encoder hierarchically so that the significant information can obtain strong protection. After UEP, the coded bit streams are combined to Y and modulated, then transmitted into the noisy channel. In receiver end, the received data streams are correspondingly demodulated, UEP decoded, SPIHT decoded, inverse DWT (IDWT) and the image would be reconstructed.

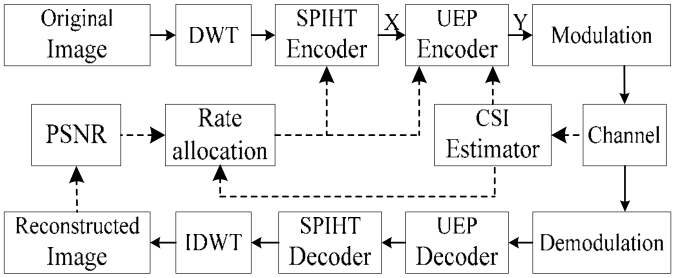


Fig. 10. Block diagram of proposed JSCC scheme based on UEP using ATC

To received data streams, the UEP decoder can be adapted to adopt various decoding algorithms and appropriate decoding iterative numbers for the different importance levels of image data streams.

(1) For received most significant data streams, UEP decoder chooses Log-MAP algorithm because of its good error correction ability. Meanwhile, properly increases decoding iterative numbers to strongly protect most significant data.

(2) For significant data, UEP decoder adopts low complicated Max-Log-MAP algorithm and moderate of the iterative numbers to reduce decoding complexity.

(3) For insignificant streams, selects lowest complexity SOVA algorithm and suitably reduces iteration numbers to further reduce computational complexity and decoding time delay.

Rate allocation in our JSCC scheme is an important part, it can optimally allocate the source CR and the channel code rates according to the calculated PSNR value of the reconstructed image and the estimated CSI condition while fixing bandwidth resource.

(1) If the calculated PSNR value is small or SNR is low, then properly increase SPIHT code rate, i.e. CR or BPP to preserve more image details. Meanwhile, select turbo coeds puncture mode to get low code rate so as to decrease the whole UEP code rate to protect image data strongly.

(2) If the PSNR is big or SNR is high, then timely reduce CR or BPP ratios to save storage size and increase UEP code rate to save channel bandwidth resource.

V. SIMULATION RESULTS AND ANALYSIS

The proposed JSCC scheme is applied to digital image communication system. Experiments are performed on 128×128 gray-scale image Lena, using 5-level wavelet decomposition based on the 9/7 tap filters, the reliability and effectiveness of the JSCC scheme was evaluated. The measure of compressed image is given by the compression ratios (CR) and the bit per pixel (BPP) ratios. CR indicates that the compressed image is stored using CR % of the initial storage size while BPP is the number of bits used to store one pixel of the image. Quality measure of the reconstructed images is given by the PSNR, where

$$PSNR = 10\log_{10}(\frac{I_{\max}^2}{MSE}) \tag{5}$$

and $I_{\max} = 255$ is the maximum pixel value for the gray-scale image when the initial pixel value is represented by 8 BPP, MSE denotes mean square error between the reconstructed image and the original image, here

$$MSE = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - I'(i,j)]^2}{MN} \tag{6}$$

M and N are the number of rows and columns of the images, I and I' are pixel value of the original image and the reconstructed image, respectively, and $0 \le i \le M-1$, $0 \le j \le N-1$.

In the transmitter, if SNR is 0-1dB, i.e. worst CSI, X1 adopts NP1-NP2-STC with K1=K2=5, X2 adopts NP1-NP2-ATC with K1=5, K2=3, X3 adopts NP1-NP2-STC with K1=K2=3. If SNR is 1-2dB, i.e. medium CSI, X1 adopts NP1-P2-ATC with K1=K2=5, X2 adopts NP1-P2-ATC with K1=5, K2=3, X3 adopts NP1-P2-ATC with K1=K2=3. And if SNR is 2-3dB, i.e. good CSI, X1 adopts P1-P2-STC with K1=K2=5, X2 adopts P1-P2-ATC with K1=5, K2=3, X3 adopts P1-P2-STC with K1=K2=3.

In the receiver, for received most significant data, the decoder chooses Log-MAP algorithm and 5 iterative. For significant data, chooses Max-Log-MAP algorithm and 4 iteration numbers. For insignificant data, selects SOVA algorithm and 3 iteration numbers. For comparison, two equal error protection (EEP) schemes using STC are also performed. In EEP, three classes bit streams all adopt NP1-NP2-STC with K=5 and 4 iteration decoding, while the decoder selects Max-Log-MAP algorithm for EEP 1 and SOVA for EEP2.

The simulation results for PSNR of JSCC with UEP and EEP in various source BPP ratios or CR and channel SNR values are listed in Table IV. The reconstructed images for JSCC with UEP and EEP in source ratio=0.5 BPP, channel SNR=1.5dB are shown in Figure 11.

From Table 4, it is obvious that the PSNR of reconstructed image for JSCC scheme with UEP using ATC is superior to EEP1 and EEP2 because the significant bit streams are strongly protected in UEP. We can see that PSNR will be better in relative higher BPP ratios with the same SNR condition, i.e. the reliability is improved, but the CR is also higher in this case, i.e. the compression effectiveness is deteriorated. We can also see that PSNR become worse in lower SNR with the same BPP ratios. To achieve the best compromise between a low CR and a good perceptual result and to adapt various channels, our JSSC scheme can optimally adjust the source BPP ratios (or CR) and channel code rates according to the calculated PSNR of the reconstructed image and the estimated SNR value.

It can be seen from Figure 11 that the reconstructed image qualities for JSCC with UEP using ATC are obviously improved and superior to EEP1 and EEP2.

Whether objective PSNR evaluation criterion or subjective visual perceptual result, the proposed JSCC scheme is effective and feasible.

TABLE IV
PSNR (dB) of JSCC with UEP and EEP in various source ratios (BPP) and channel SNR (dB)

Source Ratio (BPP)	CR (%)	Channel SNR (dB)	PSNR (dB)		
			UEP	EEP1	EEP2
0.25	3.13	0.50	24.51	19.87	18.05
		1.50	28.84	24.65	22.32
		2.50	31.62	28.02	25.88
0.5	6.16	0.50	26.79	22.11	20.33
		1.50	31.10	27.38	25.40
		2.50	34.55	31.25	29.28
0.75	9.38	0.50	29.13	25.21	22.73
		1.50	33.22	29.80	27.69
		2.50	36.81	33.65	31.44

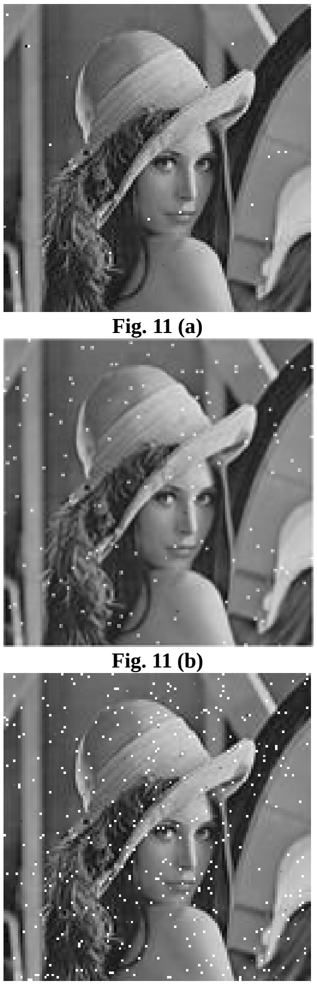


Fig. 11 (a)

Fig. 11 (b)

Fig. 11 (c)

Fig. 11. Reconstructed images with source ratio=0.5BPP and channel SNR=1.5dB (a) UEP (b) EEP1 (c) EEP2

VI. CONCLUSIONS

This paper presents an efficient JSCC design based on UEP using ATC, which can adaptively adopt different coding strategies, different interleavers of turbo codes, various decoding algorithms and appropriate decoding iterative numbers according to the different significant levels of image data streams and the varying conditions of estimated channel CSI. This scheme can also dynamically allocate the source ratios and channel code rates according to the calculated PSNR of reconstructed images and the estimated CSI. The proposed JSCC scheme can not only evidently improve the reconstructed image qualities but also enhance the reliability of the communication system with no additional bandwidth, our scheme is more adaptive and robust.

REFERENCES

[1] G. Cheung and A. Zakhor, “Joint source-channel coding of scalable video over noisy channels,” in *IEEE Int. Conf. Image Process*., vol.3, pp. 767-770, Sep. 1996.

[2] R. Hamzaoui, V. Stankovic and Z.Xiong; "Optimized error protection of scalable image bit streams [advances in joint source-channel coding for images]," *IEEE Signal Process.*, vol. 22, no. 6, pp. 91-107, Nov. 2005.

[3] L.Yao and L. Cao, "Turbo Codes-Based Image Transmission for Channels With Multiple Types of Distortion," *IEEE Trans. Signal Process.*, vol. 17, no. 11, pp. 2112-2121, Nov. 2008.

[4] C. Lan, T. Chu, K. R. Narayanan and Z. Xiong, “Scalable image and video transmission using irregular repeat–accumulate codes with fast algorithm for optimal unequal error protection,” *IEEE Trans. Commun.*, vol. 52, no. 7, pp. 1092–1101, Jul. 2004.

[5] P. G. Sherwood and K. Zeger, “Progressive image coding for noisy channels,” *IEEE Signal Process. Lett*., vol. 4, no. 7, pp. 189-191, Jul. 1997.

[6] Lei Cao, “On the unequal error protection for progressive image transmission,” *IEEE Trans. Image Process*., vol. 16, no. 9, pp. 2384-2388, Sept. 2007.

[7] G. Caire and G. Lechner, “Turbo codes with unequal error protection,” *IET Electron.. Lett*., vol. 32, no. 7, pp. 629-631, Feb. 1996.

[8] N. Thomos, N. Boulgouris and M. Strintzis, “Wireless image transmission using Turbo codes and optimal unequal error protection,” *IEEE Trans. Image Process.*, vol. 14, no. 11, pp. 1890-1901, Nov. 2005.

[9] M. Aydinlik and M. Salehi, “Turbo coded modulation for unequal error protection,” *IEEE Trans. Commun.*, vol. 56, no. 4, pp. 555-564, Apr. 2008.

[10] Y.Takeshita, M.Collins and P.Massey, “A note on asymmetric Turbo codes,” *IEEE Commun. Lett.*, vol. 3, no. 3, pp. 69-71, Mar. 1999.

[11] B.Shim, S.Choi, H.Park, S.Kim and Y.Ra, “A study on performance evaluation of the asymmetric Turbo codes,” in *IEEE Proc. ICHIT' 08*, pp. 667-671, Aug. 2008.

[12] K.Ramasamy, B.Balakrishnan and M.Siddiqi, “A new class of asymmetric turbo code for 3G systems,” *Int. J. Electron. Commun.*, pp. 447-458, Jun. 2006.

[13] H.X.Wang and S.F.Liu, "A Novel Interleaver Design for Turbo Codes," *J. South-Central University for Nationalities*, vol. 29, no. 3, pp.58-60, Sep. 2010.

[14] M.Salim and S.Shrimal, “Modified interleaver design to reduce error floor in turbo codes for wireless communication,” in *IEEE Proc. AMTA' 08*, pp. 698-701, Nov. 2008.

[15] S.Park and J.Jeon, “Interleaver optimization of convolutional turbo code for 802.16 systems,” *IEEE Commun. Lett.*, vol. 13, no. 5, pp. 339-341, May. 2009.

[16] J.Costello, J.Hagenauer, H.Imai and B.Wicker, “Applications of error-control coding,” *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2531-2560, Jul. 1998.

[17] C.Berrou, A.Glavieux and P.Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo codes,” *in IEEE Proc. ICC' 93*, pp. 1064-1070, May. 1993.

[18] J.Hagenauer, E.Offer and L.Papke, “Iterative decoding of binary block

and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 429-445, Mar. 1996.

[19] C.D.Creusere, "A new method of robust image compression based on the embedded zero-tree wavelet algorithm," *IEEE Trans. Image Process*., vol. 6, no. 10, pp.1436-1442, Oct. 1997.

[20] P. Sherwood and K. Zeger, "Progressive image coding for noisy channels," *IEEE Signal Process. Lett*., vol. 4, pp. 189-191, Jul. 1997.

[21] A. Said and W. A. Pearlman, "A new fast and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, no. 3, pp. 243–250, Jun. 1996.

Hanxin Wang, South-Central University for Nationalities, Wuhan, China.
Hanxin Wang received the B.S. degree in electronics and information engineering from Wuhan University, China in 1989, and finished the M.S. degree course in electronics and information engineering from South-Central University for Nationalities, China in 2002. Since 1989, he was a network engineer in Hua-zhong Computer System Engineering Company, China. During 2002-2003, as an invited visitor, he studied on wideband wireless communication in Institute of Information and Communication, Chonbuk National University, Korea. Since 2003, he was an associate professor in College of Electronics and Information Engineering, South-Central University for Nationalities, China. His research interests include information theory and modern coding theory, wideband wireless and mobile communication, cognitive radio network.

Cuitao Zhu, received the M.S. degree and the Ph.D. degree in communication and information system from Huazhong University of Science & Technology in 1999 and 2008, respectively. He is currently a professor in College of Electronics and Information Engineering, South-Central University for Nationalities, China. His research interests include wideband wireless communication, cognitive radio, compressed sensing.

Chengyi Xiong, received the M.S. degree in communication and information system in 2000 from South-Central University for Nationalities, and the Ph.D. degree from Huazhong University of Science & Technology in 2006. He is currently a professor in College of Electronics and Information Engineering, South-Central University for Nationalities, China. His research interests include signal processing, compressed coding of image and video, compressed sensing.

Shaoping Chen, received the M.S. degree in communication and information system in 1990 from Wuhan University, and the Ph.D. degree from Huazhong University of Science & Technology in 2004. He is currently a professor in College of Electronics and Information Engineering, South-Central University for Nationalities, China. His research interests include high speed wireless communication, digital signal processing, MIMO system, OFDM technique.

Efficient and Format-Compliant Video Encryption Algorithm in Compressed Domain for H.264/AVC

Li ZHUO, Niansheng MAO, Haojie SHEN, Jing ZHANG, Xiaoguang LI

Signal and Information Processing Laboratory, Beijing University of Technology, Beijing, China

zhuoli@bjut.edu.cn, mns150@sohu.com, 13810761814 @139.com, zhj@bjut.edu.cn, lxg@bjut.edu.cn

Abstract—**In this paper, an efficient video encryption scheme is proposed for protecting H.264 bitstream. The issues on the compressed domain video encryption have been pointed out and fully addressed. In the proposed scheme, only the most significant bits for video reconstruction in H.264 bitstream are extracted and encrypted, to optimize the trade-off between security level and computational complexity. For intra-frames, only the codewords of intra4×4 prediction mode and the sign bits of the low frequency DCT coefficient are encrypted. For inter-frames, the info_suffix of motion vector difference (MVD) are encrypted. Owing to the proposed scheme is independent of the compression process, thus does not need to modify the structure of H.264 standard codec. Experimental results show that the proposed scheme exhibits significant computational efficiency and reliable security, can resist not only perceptual attacks but also brute-force attacks. Furthermore, it adds a little memory overhead. Therefore, the proposed scheme will be well suited for real-time video applications and resource-limited systems such as smartphone and wireless sensor network.**

Index Terms—**Video encryption, Security, H.264, Bitstream, Compressed domain**

I. INTRODUCTION

With the rapid development of computer and network technology, multimedia systems such as videophone, video surveillance and telemedicine, have been widely used. The security and privacy of multimedia content are becoming more and more prominent. Conventional cryptographic algorithms such as data encryption standard (DES) [1] and advanced encryption standard (AES) [2] are difficult to be applied directly to multimedia content duo to the large volume of data and real-time video requirements. Furthermore, in the case of the wireless mobile terminals, limited processing power, memory and bandwidth always fail to meet the encryption processing overhead. Thus, efficient video encryption schemes need to be designed.

In real-world applications, a video encryption scheme should take various requirements into account, such as security, computational efficiency, compression efficiency, format-compliance and so forth. Different video applications require variable levels of security. For example, for Video on Demand (VoD) or pay-TV, low security is often required, and even nonpaying users are allowed to access low quality versions to promote them to buy high quality versions, whereas for military secrets or financial information, strict security is demanded to completely prevent the unauthorized access. The computational efficiency means that the encryption or decryption process can not cause too much time delay, to meet the requirements of real-time applications. Video compression is employed to reduce the storage space and save bandwidth, so that the encryption process should have a least impact on the compression efficiency. The format-compliance, also known as syntax-compliance [3], means that the encryption scheme should do not change the syntax structure of the compressed bitstream, thus ensures features like cutting, copying, adding or removing, and ability of the encrypted bitstream still can be decoded by a standard decoder.

In recent years, many video encryption algorithms have been proposed. As pointed out in [4], these algorithms according to their association with video compression can be classified into two categories, called compression-joint encryption algorithms and compression-independent encryption algorithms. For the former, the encryption algorithms are embedded in a certain step of the compression process. For example, some algorithms permute or scramble the residual coefficients after the Discrete Cosine Transform (DCT) [5]-[7], some algorithms encrypt the signs of DCT coefficients or motion vector difference (MVD) after quantization [8], [9], and some algorithms selectively encrypt intra-prediction modes, DCT coefficients, and MVD during the entropy coding [10]-[12].

Manuscript received May 3, 2012. This work was sponsored by the Program for New Century Excellent Talents in University, the Excellent Science Program for the Returned Overseas Chinese Scholars of Ministry of Human Resources and Social Security of China, Scientific Research Foundation for the Returned Overseas Chinese Scholars of MOE.

Li ZHUO is currently a professor of the Beijing University of Technology, Beijing, China (email: zhuoli@bjut.edu.cn)

Niansheng MAO was a master student of the Beijing University of Technology, Beijing, China (email: mns150@sohu.com)

Haojie SHEN is currently a master student of the Beijing University of Technology, Beijing, China (email: 13810761814 @139.com)

Jing ZHANG is currently an associate professor of the Beijing University of Technology, Beijing, China (email: zhj@bjut.edu.cn)

Xiaoguang LI is currently an associate professor of the Beijing University of Technology, Beijing, China (email: lxg@bjut.edu.cn)

As these encryption algorithms are all accomplished before the last step of the video compression process, all the encrypted bitstreams can be decoded by a standard decoder without being decrypted, while only obtain the unintelligible video. However, encrypting or scrambling the DCT coefficients during the compression process usually destroys the inherent energy impact capability of the DCT transform, resulting in low compression efficiency.

Differently, for the compression-independent encryption algorithms, the compression and encryption process are carried out separately. These algorithms often directly encrypt the compressed bitstream, also known as compressed domain video encryption. In [13], the odd indexed bytes in video bitstream are firstly encrypted with a conventional cryptographic algorithm, and used as keys to XOR with the even indexed bytes. In [14], the bitstream according to their importance for decoding are divided into five types, and the first three are encrypted whereas others remain. Both of the above algorithms can ensure enough security, but are all of low computational efficiency and loss the format-compliance. In [3], the codewords of DCT coefficients and MVD in compressed bitstream are shuffled. In [15], the codewords of intra-prediction mode are encrypted. Both of them demonstrate high computational efficiency and maintain the format-compliance, but are of low security. As can be seen, the various existing compressed domain encryption schemes cannot optimize the trade-off between security level and computational complexity, and are often difficult to maintain the format-compliance. Therefore, the compressed domain video encryption algorithms need to be further studied.

In this paper, we propose an efficient compressed domain video encryption scheme for protecting H.264 bitstream. The proposed scheme directly extracts the most significant bits for video reconstruction in H.264 bitstream, concatenates them in an appropriate way to form a sub-bitstream, and then encrypts the sub-bitstream with a conventional cryptographic algorithm such as AES. After the encryption process, the encrypted bits are put back into their original positions.

The rest of this paper is organized as follows. Section II analyses the H.264 bitstream syntax structure. Details of the proposed video encryption scheme are described in Section III. The performance of the proposed scheme is discussed in Section IV. Section V presents some conclusions.

II. H.264 Bitstream Syntax Structure

H.264/AVC [16] is the state-of-the-art video coding standard. Compared with the previous standards such as MPEG-2, H.263, it not only has excellent compression performance, but also has a “network-friendly” bitstream structure. In general, the basic unit of the H.264 bitstream is variable length code (VLC) codewords and fixed length code (FLC) codewords, which are formed by a number of bits and represent different information types. These codewords play different roles in the decoding process. For example, the codewords of the header include synchronization information, and the codewords of MVD contain video motion information and so forth. In order to improve the encryption scheme pertinence and efficiency, the structure of the H.264 bitstream will be firstly analysed in this section.

To achieve higher compression efficiency, the H.264 bitstream is organized with a hierarchical structure, as shown in Figure 1. The H.264 bitstream can be divided into a series of Network Abstraction Layer (NAL) units. Each NAL unit contains NAL header information and a Raw Byte Sequence Payload (RBSP), which can be Sequence Parameter Set (SPS), Picture Parameter Set (PPS) or a coded slice. Among them, the SPS contains SPS_id, profile and level, the number of reference frames, image width and height, and so on. The PPS contains PPS_id, SPS_id, entropy coding mode, reference frame index, the initial quantization parameter (QP), and so on. The SPS and PPS do not correspond to a particular sequence or image, in other words, an SPS can be used for multiple sequences and a PPS can also be used for multiple images. The coded slice consists of slice header (including slice type, PPS_id and QP offset) and a number of macroblock (MB) data.

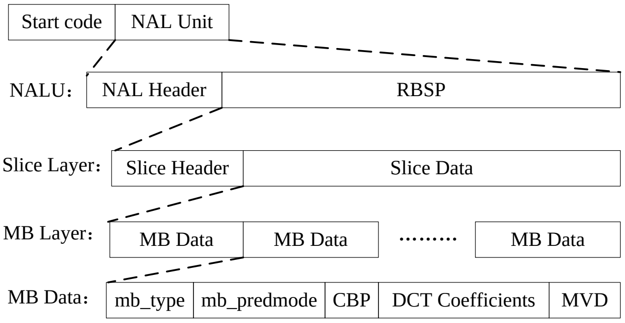


Fig. 1. H.264 bitstream hierarchical structure.

For video encryption, the SPS, PPS and slice header only provide nominal security, as these coding parameters do not contain too much information and usually have a fixed format. The MB data can be classed into intra-macroblock data (including MB_type, intra-prediction mode, coded block pattern (CBP) and DCT coefficients) and inter-macroblock data (including MB_type, inter-prediction mode, CBP, MVD and DCT coefficients). Among them, the DCT coefficients contain video texture information, the MVD contain video dynamic information, and the intra-prediction mode indicates the predicted direction. All these information are the most important for video reconstruction. Therefore, in order to obtain high security, the codewords of intra-prediction mode, DCT coefficient, and MVD in H.264 bitstream should be encrypted.

III. The Proposed Encryption Scheme

Based on the above analysis, an efficient compressed domain encryption scheme is proposed in this section. For intra-prediction mode, the codewords are encrypted with IPME algorithm [15], for the low frequency DCT coefficients of intra-frames, only the sign bits are extracted and encrypted, and for the motion vector difference, the info_suffix of the codewords are encrypted. The proposed scheme is shown in Figure 2.

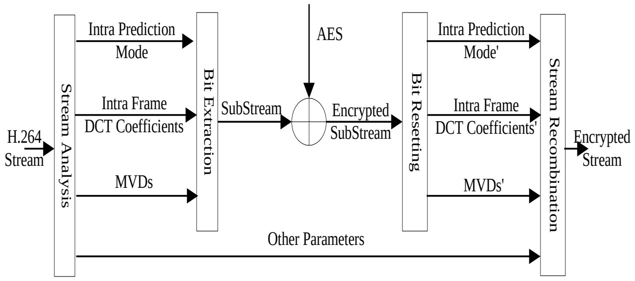


Fig. 2. Diagram of the proposed encryption scheme.

A. Intra-Prediction Mode Encryption

In H.264 bitstream, the intra4×4 prediction mode is denoted by two syntax elements, prev_intra4×4_pred_mode with 1bit and rem_intra4×4_pred_mode with 3 bits. If the prev_intra4×4_pred_mode is set to '1', the current block uses the most_probable_mode, which is the minimum of the prediction modes of its two neighboring upper and left blocks, and the rem_intra4×4_pred_mode is not adopted. Otherwise, the prev_intra4×4_pred_mode is set to '0', and the prediction mode of the current block is presented by the rem_intra4×4_pred_mode.

In IPME algorithm [15], only the codewords of the rem_intra4×4_pred_mode in H.264 bitstream are encrypted. The algorithm is simple and computationally efficient, but lacks of security due to the limited encryption space. In the improved algorithm [17], in order to obtain higher security, when the prev_intra4×4_pred_mode is set to '1', the encryption operation is to reset it to '0' and inserts 3 bits chaotic sequence as the rem_intra4×4_pred_mode, and all the intra4×4 prediction modes are encrypted by chaotic pseudo random sequence. However, the improved algorithm significantly increases the computational complexity, and bears a large amount of processing overhead and memory requirements. Thus, the codewords of intra4×4 prediction modes are encrypted with IPME in the proposed scheme.

Differently, the intra16×16 prediction modes are jointly encoded with the luma and chroma CBP using the unsigned Exp-Golomb entropy coding. The CBP indicates which blocks within a macroblock contain DCT coefficients, so that its values should not be changed during encryption, otherwise the encrypted bitstream will loss the format-compliance. Thus, the proposed scheme does not encrypt the intra16×16 codewords.

B. DCT Coefficients Encryption

The DCT coefficients in H.264 baseline profile are encoded with the context-based adaptive variable length coding (CAVLC). The encoding process can be described as follows [16]:

- Encoding the number of coefficients and trailing ones (coeff_token),
- Encoding the sign of each trailing ones,
- Encoding the levels of the remaining non-zero coefficients,
- Encoding the total number of zeros before the last coefficient, and
- Encoding each run of zeros.

After the CAVLC process, the residual data is represented by numerous coding parameters such as the number of nonzero coefficients and trailing ones (coeff_token), the sign of trailing ones (TrailingOnes), the remaining nonzero coefficients (NonCoeff), the total number of zeros before the last coefficient (TotalZeros) and each run of zeros (run_before). Since it is context adaptive, in order to maintain the format-compliance, the context adaptive property should not be destroyed during the encryption. In other words, the codewords of coeff_token, TotalZeros and run_before should not be changed. More specifically, only the sign bits of NonCoeff codeword and the codewords of TrailingOnes can be encrypted. For optimize the tradeoff between security and computational complexity, only the sign bits of the low frequency DCT coefficients of intra-frames are encrypted in the proposed scheme.

C. MVD Encryption

In H.264, each MVD is independently coded by the signed Exp-Golomb entropy coding. It means that the MVD codewords in H.264 bitstream are mutually independent. Furthermore, each MVD codeword in H.264 bitstream is constructed as [M Zeros][1][INFO], where INFO is a M-bit suffix information called info_suffix. Here, the MVD level is $X = 2^M + INFO - 1$ and the last one bit of the info_suffix is the MVD sign. Therefore, the entire info_suffix of the MVD codewords should be extracted and encrypted.

IV. Performance Analysis

In our experiments, a variety of standard video sequences in CIF and QCIF format, such as "Akiyo", "Foreman", "Mobile", "Football", "Tempete" and "Silent" are applied to demonstrate the performance of the proposed encryption scheme. Each video sequence contains 150 frames. These videos are all encoded by JM86 with a frame rate 15Hz, and the intra-frame period is set as 15. The performance of the proposed scheme, such as security, computational complexity and memory requirement, are analysed as follow.

A. Security

For video encryption, the security requires not only cryptographic security but also perceptual security. The former one specifically deals with the security against cryptographic attacks, for example, brute-force attacks. The perceptual security means that, whether or not the perceptual attacks such as the error-concealment-based attacks and the replacement attacks are used, the encrypted video remain appears unintelligible to a viewer without being decrypted.

1) Perceptual security

As we know, the most significant bits for video reconstruction in H.264 bitstream are encrypted in the proposed scheme. That is to say, the proposed scheme will make it difficult to recognize the encrypted videos. Figure 3 shows the encrypted results of several videos. It is obvious that all the encrypted videos appear unrecognizable. Besides, the quality of the encrypted videos is measured with the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity (SSIM) respectively. As can be seen from Table 1, for the encrypted videos, the PSNR value is all about 10 dB and the SSIM value is less than 0.3, both of them are much lower compared with the corresponding original videos. Thus, the proposed scheme can achieve a high perceptual security.

TABLE I
The encrypted videos quality

Size	**Video**	**PSNR-Y(dB)**		**SSIM**	
		Original	**Encrypt**	**Original**	**Encrypt**
QCIF	Akiyo	38.54	11.25	0.969	0.273
	Carphone	37.24	8.65	0.965	0.238
	Hall	37.43	9.38	0.971	0.208
	Silent	36.01	7.64	0.947	0.224
CIF	Foreman	36.82	7.81	0.936	0.257
	Football	36.53	12.77	0.933	0.282
	Harbour	34.41	9.99	0.962	0.057
	Tempete	34.67	9.01	0.961	0.094
	City	34.94	10.51	0.931	0.159

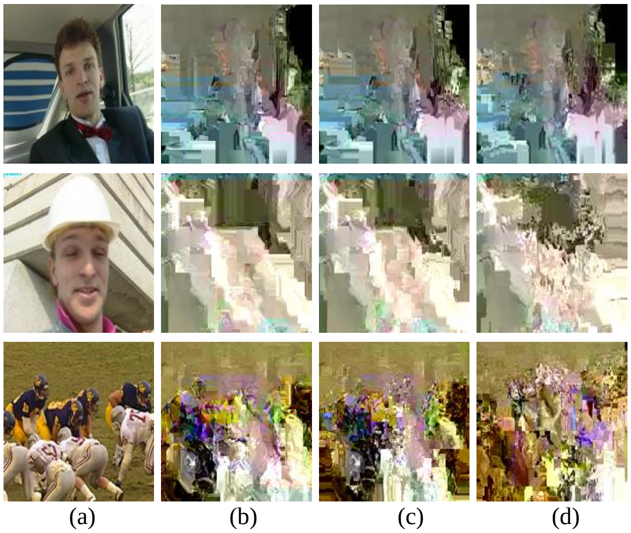


Fig. 3. The encrypted results of several videos. The column (a) is the original frames, the column (b) is the encrypted intra-frames, and the column (c) and (d) are the firth and last inter-frames in a GOP respectively.

2) Perceptual attacks

The error-concealment-based attack means that the attackers usually treat the encrypted data as bit-error or packet-loss, and then try to minimize the impact on video reconstruction as a result of the encryption by using various error-concealment techniques. However, it is very difficult for an attacker to identify the encrypted parts from a format-compliant encrypted bitstream and therefore the error-concealment-based attacks become invalid. The replacement attack is to attempt to recover the encrypted information and make it more visually acceptable by replacing the encrypted data with some particular data. For example, the encrypted intra-prediction modes can be replaced by the most_probable_mode (the minimum of the prediction modes of its neighbouring blocks), since the adjacent blocks often have the same intra-prediction modes. Figure 4 shows the recovered frames with replacement attacks. As can be seen, the recovered frames remain unintelligible after replacement attacks. Therefore, the proposed scheme is secure enough against the replacement attacks.

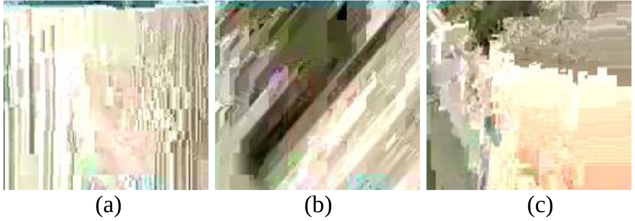


Fig. 4. The recovered frames with replacement attacks. (a) and (b) are the recovered frames by replacing the intra-prediction mode, (c) is the recovered frame by replacing the sign bits of MVD.

3) Brute-force attacks

For video encryption algorithms, the brute-force attack is not only based on cryptographic system analysis trying to enumerate all the system keys but also to enumerate the intra-prediction modes, DCT coefficients and MVD. Since the AES supports 128, 192 and 256 bits key length, the minimum brute-force space is 2^{128}. That is to say, the brute-force space for each encrypted frame using the proposed scheme is 2^{128}. It is too large for attackers to break the cryptographic system. In addition, the brute-force space of the intra-prediction mode, the sign of DCT coefficient and MVD are 2^3, 2 and 2^R (R is the length of the info_suffix of MVD), respectively. Therefore, for a W×H size frame, the brute-force space of intra-frame is $S_{intra} = [2^3 \cdot 2^L]^M, L \ge 0, M = WH/256$, where L is the number of the encrypted low frequency DCT coefficients, and the brute-force space of inter-frame is $S_{inter} = [2^3]^{N_1} \cdot [2^R]^{2N_2}, R \ge 1$, $N_1 + N_2 = WH/256$, where N_1 and N_2 are the number of intra-coded macroblocks and inter-coded macroblocks respectively. Taking QCIF (W×H =176×144) for example, the brute-force space is $S_{intra} \ge 2^{297}$ and $S_{inter} \ge 2^{198}$. Similarly, this brute-force space is also large enough to resist brute-force attacks.

B. Computational complexity

The proposed scheme can be achieved after three steps, including bit extraction, encryption and bit resetting. Hence, the computational complexity of the proposed scheme will mainly depend on these three steps. In the bit extraction process, the codewords of intra-prediction mode, DCT coefficients and MVD can be quickly detected according to the H.264 bitstream hierarchical structure, and then the bits which should be encrypted are directly extracted from these codewords based on the corresponding entropy coding without being decoded firstly. For example, the info_suffix of MVD can be extracted according to the M-bit leading zeros. The encryption time consumption depends on the data volumes to be encrypted. Table 2 gives the ratio between the encrypted data and the entire bitstream (Edr) of various standard videos. The table clearly shows that all the Edr are no more than 15%. To save the bit resetting time consumption, the location information of the encrypted bits is recorded during the bit extraction processing, so that the encrypted bits can be easily put back into their original position just like a replacement. Thus, the computational complexity of the proposed scheme will be very low.

In our experiments, the Encryption-to-compression time ratio (Etr) and the Decryption-to-decompression time ratio (Dtr) are tested. Table 3 gives the experimental results of various videos, where the proposed scheme is called PEH264. As can be seen, most of the Etr of the proposed scheme is no more than 1%, and the Dtr of the proposed scheme is also no more than 5% and 10% for QCIF and CIF videos respectively. In addition, the Etr and Dtr of the proposed scheme are all superior in comparison to the SEH264 algorithm [11]. All in all, the proposed scheme obtains significant computational efficiency. Thus, it will be well suited for real-time video applications.

TABLE II
The Edr testing results

Size	Video	Edr	Size	Video	Edr
QCIF	Akiyo	10.02%	CIF	Akiyo	9.60%
	News	9.35%		Mobile	10.46%
	Mother	8.68%		Tempete	7.03%
	Salesman	11.76%		Football	11.09%
	Foreman	10.76%		Foreman	9.82%

TABLE III
The Testing Results of Computational Cost

Video	Size	Time ratio			
		Encryption/ Compression		Decryption/ Decompression	
		SEAH264	PVEA	SEAH264	PVEA
Foreman	QCIF	0.9%	0.5%	5.2%	2.9%
Akiyo	QCIF	1.1%	0.6%	4.9%	4.6%
Mother	QCIF	0.7%	0.3%	5.9%	2.8%
Akiyo	CIF	0.7%	0.4%	6.1%	3.6%
Foreman	CIF	1.0%	0.3%	6.2%	4.3%
Mobile	CIF	0.9%	0.8%	6.2%	5.8%

C. Memory requirement

Generally, the larger amount of data is processed in encryption, the more memory is required. Therefore, the memory requirement of the proposed scheme can be measured by the amount of the encrypted data. Figure 5 shows the ratio between the encrypted data and the corresponding slice data. As can be seen, for intra-frames, the encrypted data is about 15% of the corresponding slice data, and for inter-frames, the ratio is only about 5%. That is because, considering intra-frames are more important than inter-frames, the proposed scheme provides enhanced encryption to this kind of information. All in all, compared with the existing encryption schemes, the proposed scheme adds less overhead of memory requirement.

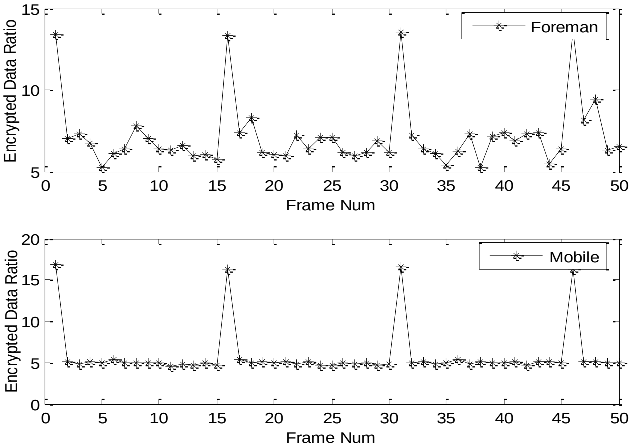


Fig. 5. The encrypted data ratio versus frame number

V. CONCLUSION

In this paper, an efficient video encryption scheme in H.264 compressed domain has been proposed. Firstly, the hierarchical structure of the H.264 bitstream is analysed, to detect the most significant bits for video reconstruction in H.264 bitstream. Then, the rem_intra4×4_pred_mode of the intra-prediction mode codewords, the sign bit of the low frequency DCT coefficients of intra-frames and the info_suffix of the MVD codewords are directly extracted and encrypted with the AES algorithm. Experimental results show that the proposed scheme exhibits reliable perceptual security, can secure against not only replacement attacks but also brute-force attacks, and meanwhile obtains significant computational efficiency. Furthermore, it maintains the format-compliance to the H.264 standard decoder and has no impact on the compression ratio. Thus, the proposed scheme will be well suited for real-time video applications and resource-limited systems such as smartphone and wireless sensor network.

REFERENCES

[1] Data Encryption Standard (DES), FIPS PUB 46, Jan. 1977.
[2] Advanced Encryption Standard (AES), FIPS-PUB 197, Nov. 2001.

[3] J. Wen, M. Severa, W. Zeng, *et al*, “A format-compliant configurable encryption framework for access control of video,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 6, pp. 545-557, Jun. 2002.

[4] F. Liu and H. Koenig, “A survey of video encryption algorithms,” *Computers and Security*, vol. 29, pp. 3-15, Feb. 2010.

[5] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently,” *Proceedings of the 4th Multimedia Conference (ACM Multimedia 96)*, pp. 219-229, Boston, MA, USA, Nov. 1996.

[6] A. S. Tang and W. C. Feng, “Efficient multi-layer coding and encryption of MPEG video streams,” *IEEE International Conference on Multimedia and Expo.*, vol. 1, pp. 119-122, Aug. 2000.

[7] W. Zeng and S. Lei, “Efficient frequency domain selective scrambling of digital video,” *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 118-129, Mar. 2003.

[8] C. Shi and B. Bharqava, “An Efficient MPEG video encryption algorithm,” *Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems*, pp. 381-386, Oct. 1998.

[9] C. Shi, S. Wang, and B. Bhargava, “MPEG video encryption in real-time using secret key cryptography,” *In Proc. of PDPTA’99*, Las Vegas, Nevada, pp.2822-2828, 1999.

[10] C. P. Wu and C. J. Kuo, “Design of integrated multimedia compression and encryption systems,” *IEEE Transactions on Multimedia*, vol. 7, no. 5, pp. 828-839, Oct. 2005.

[11] S. Lian, Z. Liu, Z. Ren and H. Wang, “Secure advanced video coding based on selective encryption algorithms,” *IEEE Transactions on Consumer Electronics*, vol. 52, no. 2, pp. 621-629, May 2006.

[12] J. Zhou, Z. Liang, Y. Chen and O. C. Au, “Security analysis of multimedia encryption schemes based on multiple Huffman table,” *IEEE Signal Processing Letters*, vol. 14, no. 3, pp. 201-204, Mar. 2007.

[13] L. Qao and K. Nahrstedt, “A new algorithm for MPEG video encryption,” *Proceedings of the First International Conference on Imaging Science, Systems and Technology (CISST’97)*, pp. 21-29, Las Vegas, Nevada, July 1997.

[14] T. Shi, B. King and P. Salama, “Selective encryption for H.264/AVC video coding,” *In SPIE International Society for Optical Engineering (San Jose, CA, USA)*, vol. 6072, pp. 171-179, Feb. 2006.

[15] J. Ahn, H. Shim, B. Jeon and I. Choi, “Digital Video Scrambling Method Using Intra Prediction Mode,” *Advanced in Multimedia Information Processing PCM2004*, vol. 3333, pp. 386-393, Dec. 2004.

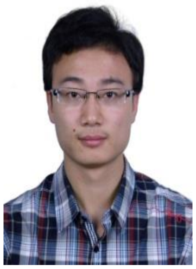
[16] T. Wiegand, G. J. Sullivan, G. Bjntegaard, *et al*, “Overview of the H.264/AVC video coding standard,” *IEEE Tran. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560-576, July 2003.

[17] J. Jiang, S. Xing and M. Qi, “An intra prediction mode-based video encryption algorithm in H.264,” *International Conference on Multimedia Information Networking and Security (MINES 2009)*, pp. 478-482, Hubei, China, Nov. 2009.

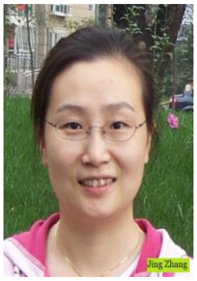
[18] Y. Mao, and M. Wu, “A joint signal processing and cryptographic approach to multimedia encryption,” *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 2061-2075, July 2006.

Li ZHUO received the B.E degree in Radio Technology from the University of Electronic Science and Technology, Chengdu, China, in 1992, the M.E degree in Signal & Information Processing from the Southeast University, Nanjing, in 1998, and the PH.D degree in Pattern Recongnization and Intellectual System from Beijing University of Technology, in 2004. She has been a professor in Beijing University of Technology since 2007. She has published over 160 research papers and authored 4 books. Her research interest includes image/video coding and transmission， multimedia content analysis, Multimedia information security.

Niansheng MAO received the B.E degree in Electronic and Information Engineering from the Beijing University of Technology, Beijing, China, in 2005, the M.E degree in Information and Communication Engineering from the Beijing University of Technology, Beijing, China, in 2012. His research interest includes video coding, scalable video coding, multimedia information security.



Haojie SHEN received the B.E degree in Electronic and Information Engineering from the Beijing University of Technology, Beijing, China, in 2011. He is currently pursuing the M.E degree in Information and Communication Engineering from the Beijing University of Technology, Beijing, China. His research interest includes video coding, multimedia information security.



Jing ZHANG received the Ph.D degree from Beijing University of Technology. She is currently an associate professor and a master supervisor at Beijing University of Technology-China and the Signal & Information Processing Lab. Her research interests include image/video processing, retrieval.

Xiaoguang LI was born in Beijing, China. He received the B.E and Ph.D degrees in Electronic Engineering from the Beijing University of Technology, Beijing China, in 2003 and 2008 respectively. He is currently an Associate Professor and master student supervisor of the Beijing University of Technology. His research interests include image and video processing and computer vision.

A Method for Evaluation of Quality of Service in Computer Networks

Tomasz Bujlow, Sara Ligaard Nørgaard Hald, Tahir Riaz, Jens Myrup Pedersen
Section for Networking and Security, Department of Electronic Systems
Aalborg University, DK-9220, Aalborg East, Denmark
tbu@es.aau.dk, slh@es.aau.dk, tahir@es.aau.dk, jens@es.aau.dk

***Abstract*—Monitoring of Quality of Service (QoS) in high-speed Internet infrastructures is a challenging task. However, precise assessments must take into account the fact that the requirements for the given quality level are service-dependent. The backbone QoS monitoring and analysis requires processing of large amounts of data and knowledge of which kinds of applications the traffic is generated by. To overcome the drawbacks of existing methods for traffic classification, we proposed and evaluated a centralized solution based on the C5.0 Machine Learning Algorithm (MLA) and decision rules. The first task was to collect and to provide to C5.0 high-quality training data divided into groups, which correspond to different types of applications. It was found that the currently existing means of collecting data (classification by ports, Deep Packet Inspection, statistical classification, public data sources) are not sufficient and they do not comply with the required standards. We developed a new system to collect training data, in which the major role is performed by volunteers. Client applications installed on volunteers' computers collect the detailed data about each flow passing through the network interface, together with the application name taken from the description of system sockets. This paper proposes a new method for measuring the level of Quality of Service in broadband networks. It is based on our Volunteer-Based System to collect the training data, Machine Learning Algorithms to generate the classification rules and the application-specific rules for assessing the QoS level. We combine both passive and active monitoring technologies. The paper evaluates different possibilities of implementation, presents the current implementation of particular parts of the system, their initial runs and the obtained results, highlighting parts relevant from the QoS point of view.**

***Index Terms*—broadband networks, data collecting, Machine Learning Algorithms, performance monitoring, Quality of Service, traffic classification, volunteer-based system.**

I. Introduction

This journal paper is the extended and revised version of [1] which was presented at the 14th International Conference on Advanced Communication Technology (ICACT 2012).

One of the most interesting challenges in today's world is how to measure the performance of computer network infrastructures, when different types of networks are merged together. In the last few years the data-oriented networks evolved into converged structures, in which real-time traffic, like voice calls or video conferences, is more and more important. The structure is composed of traditional data cable or more modern fiber links, existing Plain Old Telephone Service (POTS) lines used to provide analog services (voice telephony), or digital services (ADSL, PBX, ISDN), and nowadays also of mobile and wireless networks. There are numerous methods for the measurement of Quality of Service (QoS) in current use, which provide the measurements both on the user side and in the core of the network. Internet Service Providers are interested in centralized measurements and detecting problems with particular customers before the customers start complaining about the problems, and if possible, before the problems are even noticed by the customers.

Each network carries data for numerous different kinds of applications. QoS requirements are dependent on the service. The main service-specific parameters are bandwidth, delay, jitter, and packet loss. Regarding delay, we can distinguish strict real time constraints for voice and video conferences, and interactive services from delivery in relaxed time frame. In conversation, a delay of about 0.1 s is hardly noticeable, but 0.25 s delay means an essential degradation of transmission quality, and more than 0.4 s is considered as severely disturbing [2].

Therefore, in order to provide detailed information about the quality level for the given service in the core of the network, we need to know, what kind of data is flowing in the network at the present time. Processing all the packets flowing in a high-speed network and examining their payload to get the application name is a very hard task, involving large amounts of processing power and storage capacity. Furthermore, numerous privacy and confidentiality issues can arise. A solution for this problem can be use of Machine Learning Algorithms (MLAs), which use previously generated

Manuscript received August 1, 2012. This work was a part of a PhD project (Grant No. 8–10100) co-financed by Center for TeleInFrastruktur at Aalborg University, a global research center (see http://www.ctif.aau.dk/), Vækstforum Nordjylland, a regional development project (see http://www.rn.dk/RegionalUdvikling/Vaekstforum/), and Bredbånd Nord A/S, a regional fiber networks deliverer (see http://www.bredbaandnord.dk/).

Tomasz Bujlow is with Section for Networking and Security, Department of Electronic Systems, Aalborg University, Aalborg East, 9220 Denmark (tel: +45 5026 2494, e-mail: tbu@es.aau.dk).

Sara Ligaard Nørgaard Hald is with Section for Networking and Security, Department of Electronic Systems, Aalborg University, Aalborg East, 9220 Denmark (e-mail: slh@es.aau.dk).

Tahir Riaz is with Section for Networking and Security, Department of Electronic Systems, Aalborg University, Aalborg East, 9220 Denmark (e-mail: tahir@es.aau.dk).

Jens Myrup Pedersen is with Section for Networking and Security, Department of Electronic Systems, Aalborg University, Aalborg East, 9220 Denmark (e-mail: jens@es.aau.dk).

decision rules, which are based on some statistical information about the traffic. In our research, we used one of the newest MLAs - C5.0. MLAs need very precise training sets to learn how to accurately classify the data, so the first issue to be solved was to find a way to collect high-quality training statistics.

In order to collect the necessary statistics and generate training sets for C5.0, a new system was developed, in which the major role is performed by volunteers. Client applications installed on their computers collect the detailed information about each flow passing through the network interface, together with the application name taken from the description of system sockets. Information about each packet belonging to the flow is also collected. Our volunteer-based system guarantees precise and detailed data sets about the network traffic. These data sets can be successfully used to generate statistics used as the input to train MLAs and to generate accurate decision rules.

The knowledge about the kind of application to which the traffic belongs obtained from MLAs can be used together with traffic requirements for the given application to assess the QoS level in the core of the real network. The real traffic needs to be sampled to obtain the necessary raw statistics. Parameters like jitter, burstiness, download and upload speed can be assessed directly on the basis of information obtained from the captured traffic. To assess delay and packet loss, active measurement techniques must be involved (like ping measurements in both directions).

The remainder of this document is split into several sections, which describe in detail the system architecture and some parts of the implementation. Section II contains the overview of current methods of assessing the network QoS level. Both passive and active methods are described along with their advantages and weaknesses. Section III gives an overview of our methods, so the reader is able to understand how the particular components are built and connected with each other. Section IV describes current methods used for traffic classification in computer networks and it explains why they are not sufficient for our needs. Section V presents our new tool used for collecting and classification of the network traffic – the Volunteer-Based System (VBS). Section VI shows how the statistical parameters are obtained from the data collected by VBS. Section VII evaluates different Machine Learning Algorithms and shows why we chose C5.0 to be included in our system. Section VIII demonstrates design and implementation of the system, while Section IX summarizes the most important points.

II. Related work

During the last 20 years we have been witnesses to the subsequent and increasing growth of the global Internet and the network technology in general. The broadband and mobile broadband performance today is mainly measured and monitored by speed. However, there are several other parameters, which are important for critical business and real-time applications, such as voice and video applications or first-person shooter games. These parameters include download and upload speeds, round trip time, jitter, packet loss, and availability [3], [4].

The lack of the centralized administration makes it difficult to impose a common measurement infrastructure or protocol. For example, the deployment of active testing devices throughout the Internet would require a separate arrangement with each service provider [3]. This state of affairs led to some attempts to make simulation systems representing real characteristics of the traffic in the network. Routers and traffic analyzers provide passive single-point measurements. They do not measure performance directly, but traffic characteristics are strongly correlated with performance. Routers and switches usually feature a capability to mirror incoming traffic to a specific port, where a traffic meter can be attached. The main difficulty in passive traffic monitoring is the steadily increasing rate of transmission links (10 or 100 GB/s), which can simply overwhelm routers or traffic analyzers, which try to process packets. It forces introduction of packet sampling techniques and, therefore, it also introduces the possibility of inaccuracies. Even at 1 Gbit/s, the measurement can result in enormous amount of data to process and store within the monitoring period [3].

To overcome the heavy load in the backbone and to not introduce inaccuracies, a smart monitoring algorithm was needed. There are several approaches to estimate which traffic flows need to be sampled. Path anomaly detection algorithm was proposed in [5]. The objective was to identify the paths, whose delay exceeds their threshold, without calculating delays for all paths. Path anomalies are typically rare events, and for the most part, the system operates normally, so there is no need to continuously compute delays for all the paths, wasting processor, memory, and storage resources [5]. Authors propose a sampling-based heuristic to compute a small set of paths to monitor, reducing monitoring overhead by nearly 50 % comparing to monitoring all the existing paths.

The next proposals on how to sample network traffic in an efficient way were made on the basis of adaptive statistical sampling techniques, and they are presented in [6] and [7].

If a congestion is detected, from user's perspective it is very important to know, if the congestion is located on the local or on the remote side. If the link experiences a local congestion, the user may be able to perform certain actions, e.g. shut down an application, which consumes a lot of bandwidth, to ease the congestion. On the other hand, if the congested link is a remote link, either in the Internet core or at the server side, the back-off of the low-priority applications on the user's side is unnecessary. It only benefits the high-priority flows from other users, which compete for that link. Since this altruistic behavior is not desirable, the low priority TCP only needs to back off, when the congested link is local [8].

Detecting the location of congestion is a challenging problem due to several reasons. First of all, we cannot send many probing packets, because it causes too much overhead, and it even expands the congestion. Secondly, without router support, the only related signals to the end applications are packet losses and delays. If packet losses were completely synchronized (packets were dropped from all the flows), the problem would be trivial. In reality, the packet loss pattern is only partially synchronized [8]. Authors of [8] attempted to solve the problem of detecting the location of the congestion by using the synchronization of the behavior of loss and delay across multiple TCP sessions in the area controlled by the same local gateway. If many flows see synchronized congestion, the local link is the congested link. If the congested link is remote, it is less likely that many flows from the same host pass the same congested link at the same time. If there is only a small number of flows which see the congestion, the authors performed an algorithm based on queuing delay patterns. If the local link is congested, most flows typically experience high delays at a similar level. Otherwise, the congestion is remote [8].

Traffic can be profiled according to the protocol composition. Usually, predominance of the TCP traffic is observed (around 95 % of the traffic mix). When congestion occurs, TCP sources respond by reducing their offered load, whereas UDP sources do not. It results in the higher ratio of UDP to TCP traffic. If the proportion becomes high and the bandwidth available to TCP connections becomes too low to maintain a reasonable transmission window, the packet loss increases dramatically (and TCP flows become dominated by retransmission timeouts) [3]. Packet sizes provide insight into the type of packet, e.g. short 40-44 bytes packets are usually TCP acknowledgment or TCP control segments (SYN, FIN or RST) [3].

Active methods for QoS monitoring raise three major concerns. First, the introduction of the test traffic will increase the network load, which can be viewed as an overhead cost for active methods. Second, the test traffic can affect measurements. Third, the traffic entering ISP can be considered as invasive and discarded or assigned to a low-priority class [3].

Within an administrative domain (but not across the entire Internet), performance can be actively monitored using the data-link layer protocol below IP, as the Operations, Administration and Maintenance (OAM) procedure in ATM and MPLS networks. As a result, at the IP layer it is often desirable to measure performance using the IP/ICMP protocol. So far, most tools or methods are based on ping (ICMP echo request and echo reply messages) or traceroute (which exploits the TTL field in the header of the IP packet) [3].

Although the round-trip times measured by ping are important, ping is unable to measure the one-way delay without additional means like GPS to synchronize clocks at the source and destination hosts. Another difficulty is that pings are often discarded or low-prioritized in many ISP networks. Traceroute will not encounter this problem because UDP packets are used. However, traceroute has known limitations. For example, successive UDP packets sent by traceroute are not guaranteed to follow the same path. Also, a returned ICMP message may not follow the same path as the UDP packet that triggered it [3].

Although end-to-end performance measurements can be carried out at the IP layer or the transport/application layer, the latest is capable of measurements closer to user's perspective. The basic idea is to run a program emulating a particular application that will send traffic through the Internet. All the parameters (delay, loss, throughput, etc) are measured on the test traffic. This approach has one major drawback - custom software needs to be installed at the measurement hosts [3].

On the basis of the mentioned work we found out that the existing solutions are not sufficient for precise QoS measurements. This state of affairs motivated us to create a new system which combines both passive and active measurement technologies.

III. The overview of the methods

The flow chart of the system is shown in Figure 1. The following paragraphs contain detailed description of our methods. At first, the volunteers must be recruited from the network users. The volunteers install on their computer a client program, which captures relevant information about the traffic and submits the data to the server. On the server these data are used to generate per-application traffic statistics. The C5.0 Machine Learning Algorithm uses these statistics to learn how to distinguish between different types of applications and, later, it generates the classification rules (decision trees).

In order to assess the network QoS level in the core of the network for particular users we needed to find a method to capture the relevant traffic. The challenging task is to process significant amount of traffic in the high-speed networks. When the relevant flows are captured, per-flow statistics need to be generated. There are two kind of statistics generated at this step: One used for determining the kind of application associated with that flow, and one used for assessing the QoS level in the passive way. The system uses previously generated classification rules together with the first type of statistics to find out which application the flow belongs to. Then, on the basis of the kind of the application, the system determines ranges of values of the relevant QoS parameters. The last step is to check if the current values (obtained from flow statistics or in the active way) match the expected ones. If not, the quality of the given service is considered as degraded.

IV. The current methods for obtaining pre-classified data

There are many existing methods for obtaining pre-classified data, but none of them were feasible to deliver data required by us to obtain accurate statistics, which could be used to train Machine Learning Algorithms (MLAs). The traffic classification requires the packets to be logically grouped into some structures, which could be assigned to the particular application. The most common used structure among the classification methods is the flow defined as a group of packets, which have the same end IP addresses, ports, and use the same transport layer protocol. In this paragraph we describe the methods and evaluate their usefulness in providing data for our system.

A. Capturing raw data from the network interfaces

The first possibility is to install one application at a time on a host, and to capture its traffic by an external tool, such as Wireshark [9]. Unfortunately, this approach is very slow and it is not scalable. At first, it requires us to install

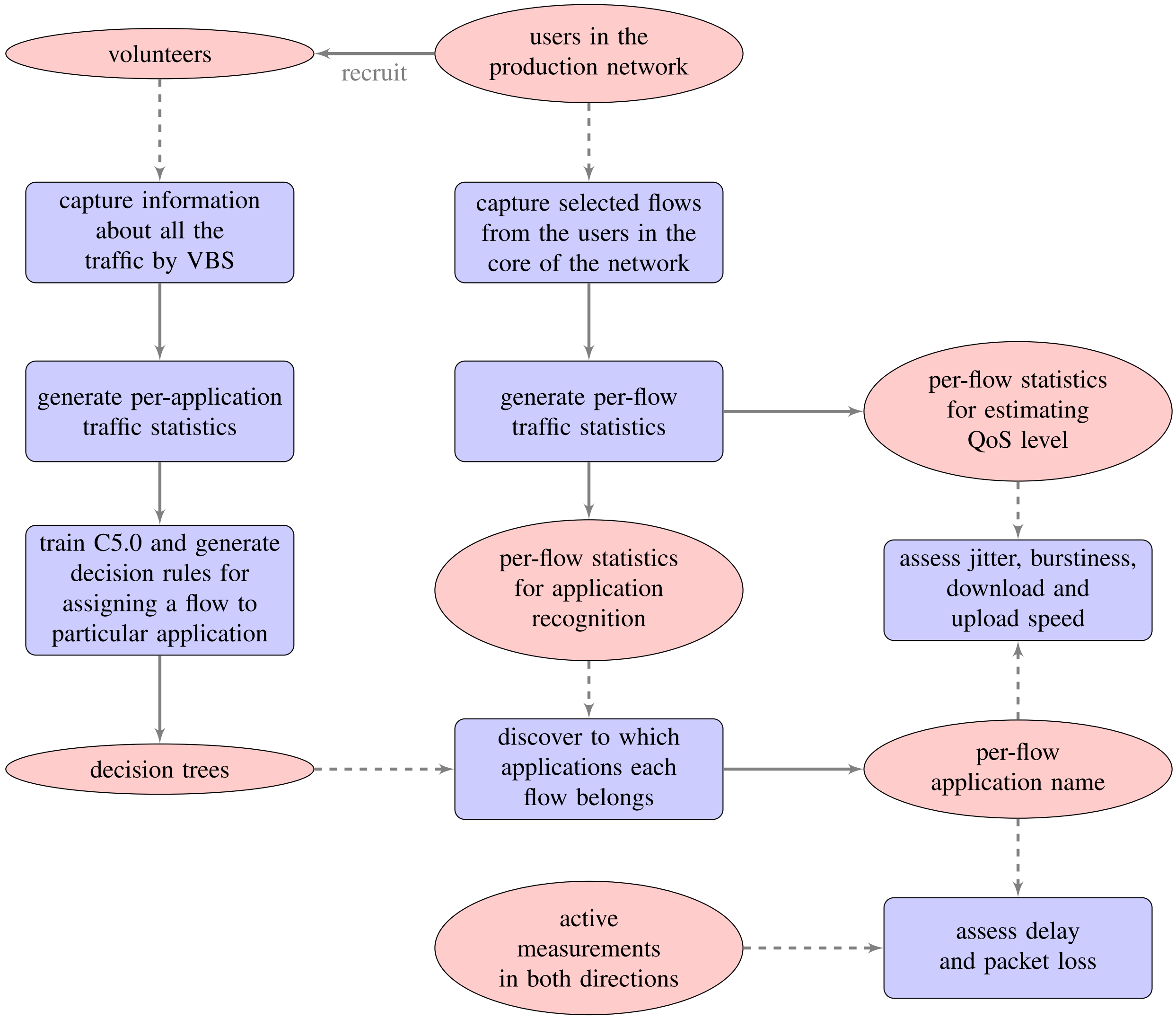

volunteers
recruit
users in the production network
capture information about all the traffic by VBS
capture selected flows from the users in the core of the network
generate per-application traffic statistics
generate per-flow traffic statistics
per-flow statistics for estimating QoS level
train C5.0 and generate decision rules for assigning a flow to particular application
per-flow statistics for application recognition
assess jitter, burstiness, download and upload speed
decision trees
discover to which applications each flow belongs
per-flow application name
active measurements in both directions
assess delay and packet loss

Figure 1. The flow chart of the system

on a host each application that generates traffic we want to capture. Before installing the application, we must uninstall all other applications that can generate any network traffic. The next drawback is that every operating system has some background processes and many of them transmit some data through the network. An example of such a process is the system updater, which can run in background. There is no simple way to recognize packets belonging to the traffic generated by the application intentionally run by us, so the captured sample contains a variable percentage of noise. Finally, some applications, for example, web browsers, can generate various types of traffic. Raw traffic capturers cannot distinguish interactive web traffic, web radio podcasts, video transmissions, or downloads of big files, performed by the same browser.

B. The classification by ports

The port-based classification [10], [11] is very fast, and it is supported on almost all the layer-3 devices in computer networks. Unfortunately, this method is limited to services, protocols, and applications, which use fixed port numbers. It means that with big probability we can correctly classify, for example, traffic generated by e-mail clients and file transfer clients using File Transfer Protocol (FTP), when they use the default ports to connect to servers. However, even in this case we have false positives and false negatives. False negatives result from non-standard ports used in this example by SMTP, POP3, or FTP servers. When a network administrator changes the port used by the given service (due to security reasons), the traffic is not classified correctly. False positives result from malicious applications, which intentionally use some well-known port numbers to be treated in the network with a priority, or to be able to transmit data at all. Such situation exists when a Torrent user runs his client on port 80, which cause the traffic to be treated as if it originated from a web server. Another big concern of port-based classification is the inability of recognizing different types of traffic using the same transport-layer protocol and the same transport-layer port. This drawback is strongly visible in the example of HTTP traffic, which can consist of data generated by interactive web browsing, audio and video streaming, file downloads, and HTTP tunneling for other protocols. Finally, the classification made by ports is unable to deal with protocols using dynamic port numbers, like BitTorrent or Skype [9], [12], [13].

C. The Deep Packet Inspection (DPI)

The big advantage of the Deep Packet Inspection (DPI) [14] is the possibility to inspect the content of the traffic. It includes both inspecting particular packets, and inspecting flows in the network as the whole. For that reason, it makes it possible to distinguish different kinds of content generated by the same application, or using the same application-layer protocol, such as HTTP. However, DPI is slow and requires a lot of processing power [9], [12]. Therefore, due to high load in today's network infrastructures, it is not feasible to run DPI in the core of the network. Speed of Internet connections provided to private users tends to increase much faster than processing power of their machines, so performing DPI on user's machines became impossible in my case. Feasibility to perform DPI on the user side does not depend only on possessing the necessary processing power, but also on the user's impression. High CPU usage tends to slow down the machine and it causes additional side-effects, for example, a howling CPU fan. For that reason, full DPI can be done only in a limited number of cases, namely on fast machines using a slow Internet connection. DPI also brings privacy and confidentiality issues, as it can reveal some highly sensitive personal data, such as information about used credit cards, logins and passwords, websites visited by the user, etc [9]. Moreover, DPI is unable to inspect encrypted traffic. Finally, DPI depends on signatures of various protocols, services, and applications, which need to be kept up to date.

D. The statistical classification

Solutions using statistical classification became quite popular during the last few years [14]. To its characteristics we can include fast processing and low resource usage. Statistical classifiers are usually based on rules, which are automatically generated from samples of data. Therefore, such kinds of classifier often make use of Machine Learning Algorithms (MLAs). Apart from all these advantages, statistical classifier have one big drawback – they need to be trained on the samples of data. So the technique assumes that we have already correctly classified data, which we can provide as the input to train the statistical classifier. For that reason, we cannot use this method to collect and classify the initial portion of data.

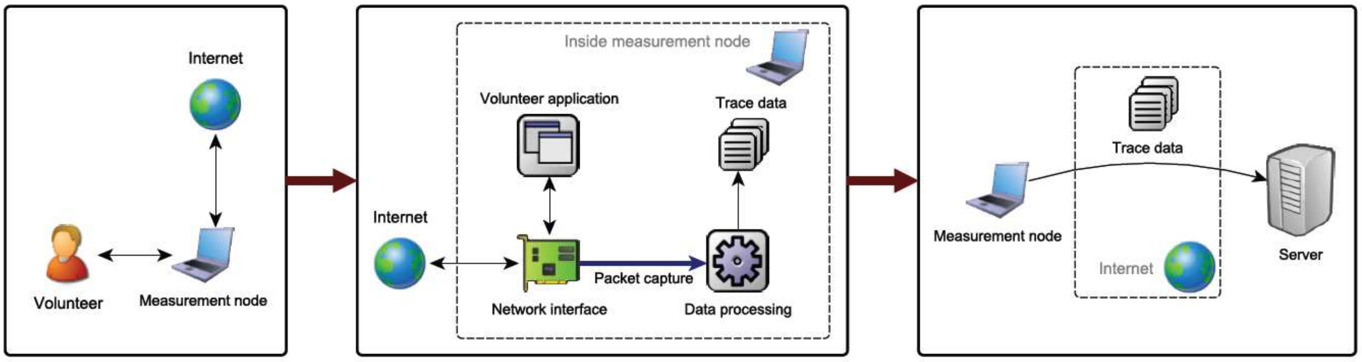
V. The Volunteer-Based System

The drawbacks of the existing methods for classification of traffic in computer networks led us to the conclusion that we need to design and build another solution. Therefore, we decided to develop a system based on volunteers, which captures the traffic from their network interfaces, and groups the traffic into flows associated with the application name taken from Windows or Linux sockets. The architecture and the prototype were described and analyzed in [15] and [16], and the first version of our current implementation was presented in [17]. Afterwards, the system was extended to support recognizing different kinds of HTTP traffic, and it was named Volunteer-Based System (VBS). The detailed description and evaluation of the extended version of the VBS system can be found in [18]. We released the system under *The GNU General Public License v3.0*, and we published it as a SourceForge project. The project website [19] contains all the information needed to use the system (binary packages, screenshots, documentation and bug tracking system) as well as to perform further development (source code, roadmap, comprehensive documentation of the source code).

The architecture of the system is shown in Figure 2. This cross-platform solution consists of clients installed on users' computers (Microsoft Windows XP and newer and Linux are supported), and of a server responsible for storing the collected data. The client registers information about each flow passing the Network Interface Card (NIC), with the exception of traffic to and from the local network. The captured information are: The start time of the flow, the anonymized identifiers of the local and the remote IP addresses, the local and the remote ports, the transport layer protocol, the anonymized identifier of the global IP address of the client, the name of the application, and the identifier of the client associated with the flow. The system also collects information about all the packets associated with each flow: The identifier of the flow to which the packet belongs, the direction, the size, the TCP flags, the relative timestamp to the previous packet in the flow, and the information about the HTTP content carried by the packet. It is worth mentioning that one flow can contain many higher-layer streams, for example, one TCP flow can contain multiple HTTP conversations. Each of these conversations can transfer different kinds of content, like web pages, audio and video streams, or downloads of big files. For that reason we extract from HTTP headers information necessary to precisely separate the HTTP streams, and we append the information about the type of the stream to the first packet of the stream.

The collected information is then transmitted to the server, which stores all the data in a MySQL database for further analysis. The system was shown in [18] to be feasible and capable of providing detailed per-application information about the network traffic. An example of stored flows on the server side is shown in Table I. The IP addresses for privacy reasons are translated by a one-way hash function and they are stored as anonymized identifiers. The information about the packets belonging to one complete TCP conversation is presented in Table II. As shown, this is an HTTP communication, during which there were transferred two files of the same type with identifier 22 (*text/html*).

The data collected during our experiments by the Volunteer-Based System were used for training the C5.0 Machine Learning Algorithm to be able to recognize traffic generated by different types of applications and different types of traffic. The first approach, focusing on distinguishing 7 different applications (Skype, FTP, torrent, web browser, web radio, America's Army and SSH) and achieving accuracy of over 99 % was described and evaluated in [20]. The second



A. Volunteer uses his computer to access the Internet

B. Packets are send through the network interface, where they are captured and processed into trace data

C. Measurement node transfers trace data to server

Figure 2. Overview of the VBS system [16]

Table I
EXAMPLE OF THE STORED FLOWS DATA

flow id	client id	start time	local IP	remote IP	local port	remote port	protocol name	global client IP	application name
1193430	4	1325445237826039	d1e0229	fb70266	48293	25395	UDP	178a02f1	uTorrent
2393417	5	1325445237826176	f4c025e	12230296	2276	80	TCP	177d02ef	chrome
1193423	1	1325445237826304	d20022b	11920285	53778	80	TCP	12350297	firefox
1484673	4	1325445237825884	d1e0229	12170293	58104	993	TCP	178a02f1	thebat
3429674	4	1325445236820017	d1e0229	14cb02b9	61159	80	TCP	178a02f1	Dropbox
3329860	1	1325445237044777	d20022b	1199028a	47801	80	TCP	12350297	plugin-container
3829589	1	1325445236797638	d20022b	124d0296	36868	80	TCP	12350297	wget
3474027	4	1325445212663601	d1e0229	14db02c2	63409	24536	UDP	178a02f1	Skype
4194793	1	1325445280781252	d20022b	1206028f	53331	22849	TCP	12350297	amule

Table II
ONE TCP COMMUNICATION STORED IN THE DATABASE

flow id	direction	packet size [B]	SYN flag	ACK flag	PSH flag	FIN flag	RST flag	CWR flag	ECN flag	URG flag	relative timestamp [μs]	content type
2784673	OUT	60	1	0	0	0	0	0	0	0	0	1
2784673	IN	60	1	1	0	0	0	0	0	0	30012	1
2784673	OUT	52	0	1	0	0	0	0	0	0	44	1
2784673	OUT	431	0	1	1	0	0	0	0	0	395	1
2784673	IN	52	0	1	0	0	0	0	0	0	30241	1
2784673	IN	527	0	1	1	0	0	0	0	0	2554	22
2784673	OUT	52	0	1	0	0	0	0	0	0	27	1
2784673	IN	539	0	1	1	0	0	0	0	0	10455	22
2784673	OUT	52	0	1	0	0	0	0	0	0	15	1
2784673	OUT	287	0	1	1	0	0	0	0	0	1383	1
2784673	OUT	52	0	1	0	1	0	0	0	0	15047	1
2784673	IN	269	0	1	1	0	0	0	0	0	16408	1
2784673	OUT	40	0	0	0	0	1	0	0	0	45	1
2784673	IN	52	0	1	0	1	0	0	0	0	13354	1
2784673	OUT	40	0	0	0	0	1	0	0	0	29	1

approach, focusing on recognizing different kinds of HTTP content (audio, video, file downloads, interactive websites) was presented in [21].

VI. OBTAINING PER-APPLICATION STATISTICS

The next step was to obtain statistical profiles of flows for different applications. Therefore, we developed a tool for calculating statistics on several traffic attributes for each flow in the database, which fulfills our requirements. The statistics include 32 attributes based on sizes and 10 protocol-dependent attributes [20]. We suspect that the attributes based on sizes are independent of the current conditions in the network (like for example congestion). All the protocol-dependent attributes are very general. Precise port numbers are not used, but only information about whether the port is well-known or dynamic. This way we avoid constructing a port-based classifier, but we can retain the information if the application model is more like client-server or peer-to-peer.

The general calculated statistics are [20]:

- number of inbound / outbound / total payload bytes in the sample.
- proportion of inbound to outbound data packets / payload

bytes.

- mean, minimum, maximum first quartile, median, third quartile, standard deviation of inbound / outbound / total payload size in the probe.
- ratio of small inbound data packets containing 50 B payload or less to all inbound data packets.
- ratio of small outbound data packets containing 50 B payload or less to all outbound data packets.
- ratio of all small data packets containing 50 B payload or less to all data packets.
- ratio of large inbound data packets containing 1300 B payload or more to all inbound data packets.
- ratio of large outbound data packets containing 1300 B payload or more to all outbound data packets.
- ratio of all large data packets containing 1300 B payload or more to all data packets.
- application: skype, ftp, torrent, web, web_radio, game, ssh.

The protocol-dependent attributes are [20]:

- transport protocol: TCP, UDP.
- local port: well-known, dynamic.
- remote port: well-known, dynamic.
- number of ACK / PSH flags for the inbound / outbound direction: continuous.
- proportion of inbound packets without payload to inbound packets: continuous.
- proportion of outbound packets without payload to outbound packets: continuous.
- proportion of packets without payload to all the packets: continuous.

The precise process of obtaining these statistics was described in detail and evaluated in [20]:

VII. Machine Learning Algorithms

In the recent literature we can find numerous approaches to use Machine Learning Algorithms to classify the traffic in computer networks. The most widely used MLA classifiers are C4.5 [9] and its modified Java implementation called J48 [12], [22]. Based on statistical analysis, MLAs have the ability to assign a particular class (like P2P) even to traffic generated by unknown applications [9]. It was also proved in [22] that the statistical parameters for encrypted and unencrypted traffic produced by the same application are similar and, therefore, the encrypted payload does not influence results of the training or the classification. The accuracy of the classification by MLAs was claimed to be over 95 % [9]–[11], [13], [14], [23]–[25]. The analysis of the related work can be found in [20].

It was found in [11] that results of the classification are most accurate when the classifier was trained in the same network as the classification process was performed. This may be due to different parameters, which are constant in the particular network, but which differ among various networks. A good example is the Maximum Transmission Unit, which can easily influence statistics based on sizes. Therefore, in our design we decided to train the classifier by volunteers in the same network as the classifier will be installed. This allows us to make a self-learning system, where a group of volunteers in the network deliver data used for training the classifier constantly improving its accuracy, while all the users can be monitored in the core using the generated decision rules. The next advantage of the design is that even if some network users cannot participate in the data collecting process because of using other operating systems or devices than supported (like MacOS, Apple or Android smartphones), they will still be able to be monitored in the core of the network because of rules created on the basis of data collected from the other users.

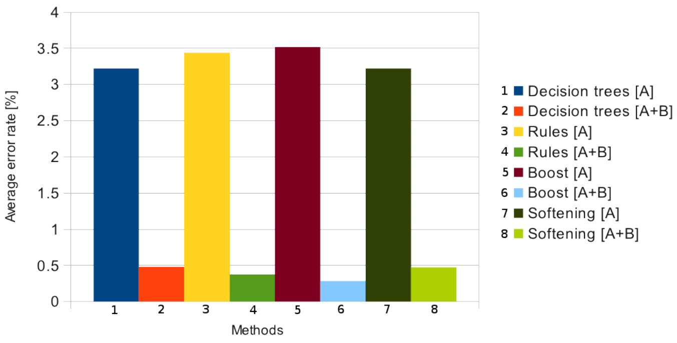


Figure 3. Average error rates of the classifiers [20]

Our system uses the C5.0 MLA, which is a successor of C4.5. It is proven to have many advantages over its predecessor, such as higher accuracy, possibilities to use boosting, pruning, weighting and winnowing attributes. Furthermore, the time to generate the decision tree or rules drastically decreased [26]. In order to test the efficiency of C5.0, we performed a set of tests during which we used various training and classification options. The training statistics were obtained from the data provided by our VBS. During our research we found relevant set of arguments and discovered that the best results were obtained using the boosted classifier. The average accuracy fluctuated between 99.3 % and 99.9 % depending on number of training and test cases and amount of data from each case. This behavior is illustrated in Figure 3. It is worth mentioning that in our experiment we considered only 7 different groups of applications and only flows longer than 15 packets. In our small-scale prototype for tests we decided to limit the number of applications and take into account Skype, FTP, torrent, web traffic, web radio traffic, interactive game traffic and SSH [20]. The limitation of the flow length was done because we needed to have at least 5 packets to generate the statistics (the first 10 packets of each flow were skipped as their behavior is different than the behavior of the rest of the flow). The detailed description of our methods and results can be found in [20]. The decision tree generated in this step can be used to classify the traffic in the real network.

VIII. The centralized monitoring solution

This paragraph presents the proposed design of the centralized monitoring solution which can be placed in any point in the network to examine network QoS.

Because of heavy load in the high-speed networks, it is not possible to monitor all the flows passing the central point at the same time. Therefore, statistics from only selected flows can be captured and passed to the C5.0. Selection of such flows can be based on two methods: Capturing one flow per user and intelligent switching between the flows. From the QoS point of view, it is important to discover problems with a particular user or to inform the user that problems experienced by him are results of problems in the remote network. If it is the user who has the problem, then the problem usually influences all the user's network activity.

Each application has some special requirements regarding network parameters. When a small congestion occurs, the service level can still be sufficient for P2P file downloads, but Skype communication may be not possible because of big jitter and delays. It is, therefore, not sufficient to monitor one random flow at a time, but we need to monitor a flow which have high quality requirements. Our solution should be built based on the following assumptions:

- Only one flow per user at a time is consistently monitored for QoS.
- Statistics for another random flow per user at a time are passed to C5.0 to discover the application.
- If the application has higher QoS requirements than the currently monitored, switch monitoring to the new flow; if not, stick to the current.
- If monitoring of the selected flow discovers problems, start monitoring few flows at a time to check if this problem lay on the user's side or on the remote side.

Because of the dynamic switching between the flows when determining the application, it is most probable that the system will not be able to capture flows from their beginning. The classifier designed by us, which use the C5.0, is able to determine the application on the basis of the given number of packets from any point in the flow [20].

Monitoring of the QoS can be done in passive or active mode. The passive mode relies mostly on time-based statistics, which are obtained directly from the flow passing the measurement point. This way, we can assess the jitter, the burstiness and the transmission speed (both download and upload). Unfortunately, it is not possible to receive information about the packet loss or the delay for other than TCP streams while using this method. For that reason, additional tools performing active measurements must be involved in the process of estimating the QoS. One option is to use the ping-based approach, as it can measure both delay and packet loss. Unfortunately, other issues can arise. Ping requests and responses are often blocked by network administrator, or their priority is modified (decreased to save the bandwidth or increased to cheat the users about the quality of the connection). Other options include sending IP packets with various TTL and awaiting *Time Exceeded* ICMP messages, which are usually allowed to be transmitted in all the networks and their priority is not changed. Active measurements must be done in both directions (from the user and from the remote side). The total packet loss and the delay can be calculated as the sum of the delays and the packet losses from both directions of the flow. Furthermore, the knowledge of the direction that causes problems can be used to assess if the problems are located in the local network or somewhere outside.

IX. Conclusion

The paper shows a novel method for assessing the Quality of Service in computer networks. Our approach involves a group of volunteers from the target network to participate in the initial training of the system, and later in the self-learning process. The accurate data obtained from the volunteers are used by the C5.0 MLA to create the per-application profiles of the network traffic as classification decision trees. The centralized measurement system uses the decision trees to determine the applications associated with flows passing through the measurement point. This knowledge allows us to precisely define the QoS requirements for each particular flow. To assess the QoS level two methods are proposed: The passive and the active one.

X. Acknowledgment

This research work was conducted in the context of a PhD project in the Section for Networking and Security in the Department of Electronic Systems at Aalborg University. We are also very grateful, for the possibility to install and test our Volunteer-Based System, to *Gimnazjum nr 3 z Oddziałami Integracyjnymi i Dwujęzycznymi imienia Karola Wojtyły w Mysłowicach*, a high school in Poland.

References

[1] Tomasz Bujlow, Tahir Riaz, Jens Myrup Pedersen, *A Method for Assessing Quality of Service in Broadband Networks*, Proceedings of the 14th International Conference on Advanced Communication Technology (ICACT 2012), IEEE 2012, pp. 826–831.

[2] Gerhard Haßlinger, *Implications of Traffic Characteristics on Quality of Service in Broadband Multi Service Networks*, Proceedings of the 30th EUROMICRO Conference (EUROMICRO'04), IEEE Computer Society 2004.

[3] Thomas M. Chen, *Internet Performance Monitoring*, Proceedings of the IEEE, vol. 90, no. 9, September 2002, pp. 1592–1603.

[4] LIRNEasia Broadband QoSE Benchmarking project, 2008. [Online]. available: http://lirneasia.net/projects/2008-2010/indicators-continued/broadband-benchmarking-qos-20/

[5] K. v. M. Naidu, Rajeev Rastogi, Bell Labs Research India, Bangalore, *Detecting Anomalies Using End-to-End Path Measurements*, IEEE INFOCOM 2008 proceedings, 2008, pp. 16–20.

[6] A. Dogman, R. Saatchi, S. Al-Khayatt, *An Adaptive Statistical Sampling Technique for Computer Network Traffic*, IEEE CSNDSP 2010, pp. 479–483.

[7] Baek-Young Choi, Jaesung Park, Zhi-Li Zhang, *Adaptive Random Sampling for Traffic Load Measurement*, IEEE International Conference on Communications, IEEE 2003, pp. 1552–1556.

[8] Shao Liu, Mung Chiang, Mathias Jourdain, Jin Li, *Congestion Location Detection: Methodology, Algorithm, and Performance*, 17th International Workshop on Quality of Service, IEEE 2009.

[9] Jun Li, Shunyi Zhang, Yanqing Lu, Junrong Yan, *Real-time P2P traffic identification*, IEEE GLOBECOM 2008 PROCEEDINGS.

[10] Riyad Alshammari, A. Nur Zincir-Heywood, *Machine Learning based encrypted traffic classification: identifying SSH and Skype*, Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009).

[11] Sven Ubik, Petr Žejdl, *Evaluating application-layer classification using a Machine Learning technique over different high speed networks*, 2010 Fifth International Conference on Systems and Networks Communications, IEEE 2010, pp. 387–391.

[12] Ying Zhang, Hongbo Wang, Shiduan Cheng, *A Method for Real-Time Peer-to-Peer Traffic Classification Based on C4.5*, 12th IEEE International Conference on Communication Technology, IEEE 2010, pp. 1192–1195.

[13] Jing Cai, Zhibin Zhang, Xinbo Song, *An analysis of UDP traffic classification*, 12th IEEE International Conference on Communication Technology, IEEE 2010, pp. 116–119.

[14] Riyad Alshammari, A. Nur Zincir-Heywood, *Unveiling Skype encrypted tunnels using GP*, IEEE Congress on Evolutionary Computation (CEC), IEEE 2010.

[15] Kartheepan Balachandran, Jacob Honoré Broberg, Kasper Revsbech, Jens Myrup Pedersen, *Volunteer-based distributed traffic data collection system*, Feb. 7-10, 2010 ICACT 2010, pp. 1147–1152.

[16] Kartheepan Balachandran, Jacob Honoré Broberg, *Volunteer-based distributed traffic data collection system*, Master Thesis at Aalborg University, Department of Electronic Systems, June 2010.

[17] Tomasz Bujlow, Kartheepan Balachandran, Tahir Riaz, Jens Myrup Pedersen, *Volunteer-Based System for classification of traffic in computer networks*, 19th Telecommunications Forum TELFOR 2011, IEEE 2011, pp. 210–213.

[18] Tomasz Bujlow, Kartheepan Balachandran, Sara Ligaard Nørgaard Hald, Tahir Riaz, Jens Myrup Pedersen, *Volunteer-Based System for research on the Internet traffic*, to appear in Telfor Journal Vol. 4 (2011).

[19] Volunteer-Based System for Research on the Internet, 2012. [Online]. Available: http://vbsi.sourceforge.net/

[20] Tomasz Bujlow, Tahir Riaz, Jens Myrup Pedersen, *A method for classification of network traffic based on C5.0 Machine Learning Algorithm*, International Conference on Computing, Networking and Communications (ICNC 2012), IEEE 2012, pp. 244–248.

[21] Tomasz Bujlow, Tahir Riaz, Jens Myrup Pedersen, *Classification of HTTP traffic based on C5.0 Machine Learning Algorithm*, to appear in Fourth IEEE International Workshop on Performance Evaluation of Communications in Distributed Systems and Wed based Service Architectures (PEDISWESA 2012).

[22] Jason But, Philip Branch, Tung Le, *Rapid identification of BitTorrent Traffic*, 35th Annual IEEE Conference on Local Computer Networks, IEEE 2010, pp. 536–543.

[23] Jun Li, Shunyi Zhang, Yanqing Lu, Zailong Zhang, *Internet Traffic Classification Using Machine Learning*, Second International Conference on Communications and Networking in China, CHINACOM ’07, 2007, pp. 239–243.

[24] Yongli Ma, Zongjue Qian, Guochu Shou, Yihong Hu, *Study of Information Network Traffic Identification Based on C4.5 Algorithm*, 4th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE 2008.

[25] Wei Li, Andrew W. Moore, *A Machine Learning Approach for Efficient Traffic Classification*, Proceedings of the Fifteenth IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems (MASCOTS’07), IEEE 2008, pp. 310–317.

[26] Is See5/C5.0 Better Than C4.5?, 2009. [Online]. Available: http://www.rulequest.com/see5-comparison.html

Tomasz Bujlow is working as a Ph.D. Student in the Section for Networking and Security (NetSec) in the Department of Electronic Systems at Aalborg University in Denmark. He received his Master of Science in Computer Engineering from Silesian University of Technology in Poland in 2008, specializing in Databases, Computer Networks and Computer Systems. Previously, he obtained his Bachelor of Computer Engineering from University of Southern Denmark in 2009, specializing in software engineering and system integration. His research interests include methods for measurement of Quality of Service and traffic classification in computer networks. He is also a Cisco Certified Network Professional (CCNP) since 2010.

Sara Ligaard Nørgaard Hald is working as a Ph.D. student in the Section for Networking and Security (NetSec) in the Department of Electronic Systems at Aalborg University in Denmark. She received her Master of Science in Computer Engineering and Management from Aalborg University in 2002, and has since worked for the Danish Defense and as a consultant specializing in enterprise architecture and cybersecurity. Research interests include threat assessments and attack detection in dedicated networks.

Tahir Riaz is working as an Assistant Professor in the Section for Networking and Security (NetSec) in the Department of Electronic Systems at Aalborg University in Denmark. He received his Master and PhD degrees in Electrical and Electronics Engineering, specializing in Network Planning and Management, from Aalborg University in 2004 and 2008, respectively. He has also worked in Nokia, Linkoping, Sweden. He has authored or co-authored over 70 papers published in conferences and journals. His research interests include access and backbone fiber optic networks, network planning and design, architecture of next generation radio of fiber networks, reliability and QoS issues in large-scale access and core network infrastructures, performance and optimization in networks.

Jens Myrup Pedersen is working as an Associate Professor and the head of the Section for Networking and Security (NetSec) in the Department of Electronic Systems at Aalborg University. His current research interests include network planning, traffic monitoring, and network security. He obtained his Master of Science in Mathematics and Computer Science from Aalborg University in 2002, and his PhD in Electrical Engineering also from Aalborg University in 2005. He is an author/co-author of more than 70 publications in international conferences and journals, and has participated in Danish, Nordic and European funded research projects. He is also a board member of a number of companies within technology and innovation.

Frequency Offset Estimation and Cell Search Algorithms for OFDMA Based Mobile WiMAX

Fakher Eldin M. Suliman, Nuha M. Elhassan, Tertiel A. Ibrahim

Sudan University of Science and Technology, Khartoum, Sudan

fakhereldinmohamed@sustech.edu, nohamohamed3@gmail.com, terteil88@yahoo.com

***Abstract*-Frequency offset estimation is an important issue in digital transceiver design, especially for coherent wireless transmission such as in WiMAX systems based on the IEEE 802.16e orthogonal frequency-division multiple access (OFDMA) due to inherited frequency and timing offset problems which contribute to the loss of the transmitted data. To overcome these problems, the transmitter and receiver must be well synchronized. In WiMAX systems, the downlink synchronization involves synchronization of carrier frequency and timing as well as identification of the preamble index. This paper introduces synchronization algorithms for frequency offset estimation and cell search. The performance of these algorithms was tested using simulation under adaptive white Gaussian noise and fading channel for different values of signal to noise ratio. Simulation provided accurate results and the frequency offset in the received frame was successfully estimated.**

***Keywords*-Carrier frequency, Cell search, Mobile WiMAX, Orthogonal frequency-division multiplexing (OFDM), Synchronization; Wireless metropolitan area network (WMAN)**

I. INTRODUCTION

In view of the requirement of providing sufficient data rate when the user is moving at high speed, the Institute of Electrical and Electronic Engineers (IEEE) has proposed the IEEE 802.16e standard to achieve a high speed broadband wireless access network for future mobile wireless communication systems [1]. The standard is widely known as WiMax, which is an acronym for Worldwide Interoperability for Microwave Access.

The WiMAX network is considered as a Wireless Metropolitan Area Network (WMAN) and is one of the Broadband Wireless Access (BWA) techniques that have emerged as a promising solution for last mile access technology. Fig.1 shows positions of different existing wireless access technologies in terms of mobility and data rate.

The IEEE 802.16e-2005 specifications define a physical (PHY) layer and a medium access control (MAC) layer for mobile and broadband wireless access systems operating at microwave frequencies below 6 GHz [2]. Actually, three different PHY layers are defined: single-carrier transmission, orthogonal frequency-division multiplexing (OFDM), and orthogonal frequency division multiple access (OFDMA). OFDMA inherits from OFDM the ability to compensate channel distortions in the frequency domain without the need of time domain equalizers. In WiMAX systems based on the IEEE 802.16e orthogonal frequency-division multiple access (OFDMA) physical layer specifications; synchronization is an essential issue. Thus without accurate synchronization algorithms, it is not possible to reliably receive the transmitted signal. Mobile WiMAX downlink (DL) synchronization involves synchronization of carrier frequency and timing as well as identification of the preamble index.

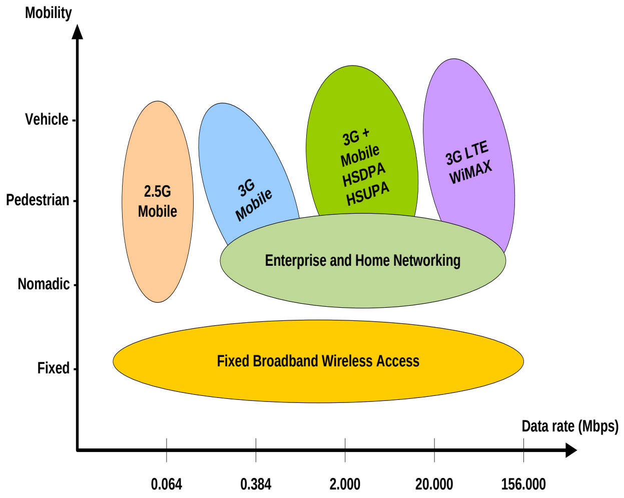


Fig. 1. Positioning of different wireless access technologies in terms of mobility and data rate.

Carrier frequency offset (CFO) may arise from the difference in natural oscillator frequencies between the base station (BS) and the mobile station (MS). However, OFDMA is extremely sensitive to timing errors and carrier frequency offsets between the incoming signal and the local oscillator used for signal demodulation.

Manuscript received 30 April, 2012.

F. M. Suliman is now with the Department of Electrical Engineering, King Khalid University, Abha, KSA (Tel: 00966551792532; e-mail: fmsuliman@kku.edu.sa)
N. M. Elhassan is with the Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan.
(e-mail: nohamohamed3@gmail.com)
T. A. Ibrahim is with the Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan.
(e-mail: terteil88@yahoo.com)

Frequency offset in an OFDM system is introduced from two sources: mismatch between the transmitted and the received sampling clocks and misalignment between the reference frequencies of transmit and receive stations. Both impairments and their effects on performance are analysed [3].

Carrier frequency errors between the transmitter and the receiver of any digital communication system increase the number of errors in the received bits. These errors result from the mismatch between the carrier frequency oscillators of the transmitter and the receiver in the RF section. Also, Doppler frequency due to the receiver's motion (up to 125 Km/hr) contributes to frequency offset [4] [5]. Carrier frequency offset has a great effect on OFDMA systems.

The OFDMA symbol depends on the subcarriers being orthogonal. Each signal of a certain subcarrier should be detected at the frequency of its maximum in the frequency domain which is exactly the value of this subcarrier, which meets a zero from the signal carried on all other subcarriers. A frequency offset will distort the signal leading to incorrect decision and interference from all other subcarriers. If the timing window slides to the left or the right, a unique phase change will be introduced to each of the subcarriers. In the frequency domain, if the carrier frequency synchronization is perfect, the receiver samples at the peak of each subcarrier, where the desired subcarrier amplitude is maximized, and the inter carrier interference (ICI) are zero. However, if the carrier frequency is misaligned by some amount d, some of the desired energy is lost, and more significantly, inter carrier interference is introduced. So it's important to detect the frequency offset that occur on the OFDM signal. The frequency offset-shift- can be [6] [7]:

- Fine frequency offset: It's a shift within one subcarrier spacing.
- Coarse frequency offset: It's a shift of multiple integer number of subcarrier spacing.

II. CYCLIC-PREFIX-BASED FINE FREQUENCY OFFSET ESTIMATION

There are a number of well-known methods that are used to estimate the frequency offset, the most efficient of which is based on exploiting time domain periodicity in the preamble. For all OFDM systems, there is always the periodicity involving the cyclic prefix. However, as will be shown later in the paper, there is a performance degradation if the system uses the cyclic prefix(CP) periodicity in estimating the frequency offset in frequency selective fading channels. That's one of the main reasons preambles are periodic in OFDM based systems. However, the preamble of the OFDMA mode of Mobile WiMAX does not have a periodic portion if it is sampled at the commonly employed Fast Fourier Transform (FFT) sampling rate. The OFDM theory requires the addition of a CP at the beginning of the OFDM symbol to allow the receiver to absorb the delay spread due to the multipath much more efficiently and to maintain frequency orthogonality. The CP occupies a duration called the guard time and is a temporal redundancy that must be taken into account in data rate computations. The CP-based estimation technique depends on the repeated time samples of the guard time. As shown in Fig.2, The cyclic prefix samples are compared to their repeated part of the preamble OFDMA symbol in the form of a correlation in time domain [8].

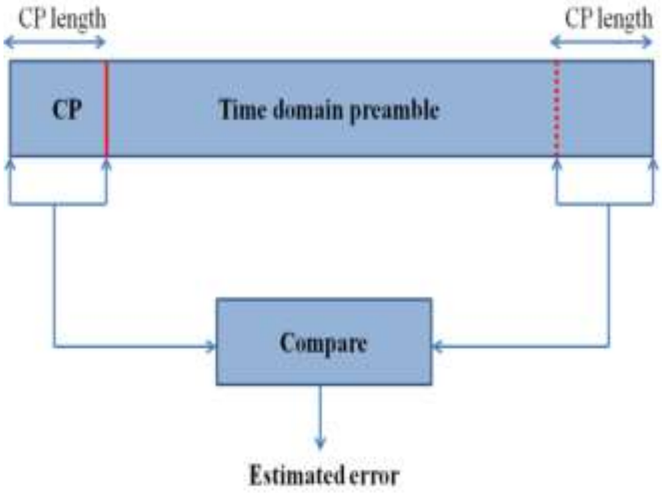


Fig. 2. Cyclic-prefix-based frequency estimation.

The proposed symbol timing technique depends on the CP nature of the OFDMA symbols. The incoming packet slides over two windows separated by fixed distance. The size of each window is the same as the used CP. When the packet is detected, the estimated start of the packet is shifted back and a correlation between the fixed windows is turned on for certain period within which the maximum correlation gives an estimate for the true symbol timing. Fig. 3 shows the illustration of this technique.

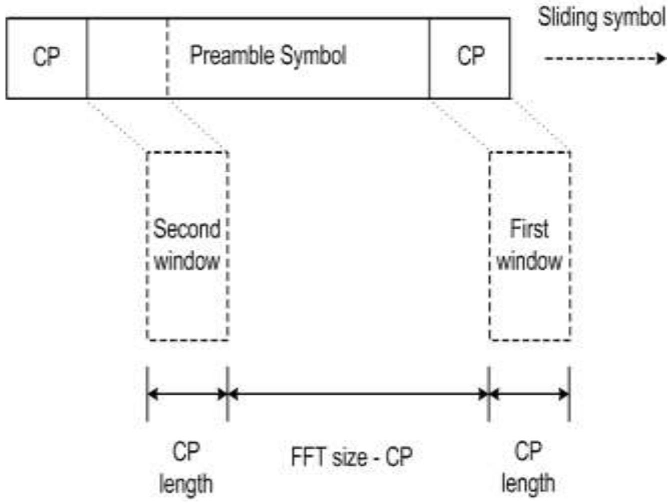


Fig. 3. Symbol timing technique.

The estimated frequency offset is proved by the following equations [9]:

$$-r_n = Sn.\exp(j2\pi\Delta fnTs) \quad (1)$$

If the number of time samples between the first time sample of the guard band and its corresponding time sample inside the OFDMA symbol is D= 1024 which is the complete FFT size, Then to estimate the frequency offset, the following algorithm may be applied:

$$\mathrm{z} = \sum_{n=0}^{l-1} \mathrm{r(n)} * \mathrm{r(n + D)} \qquad (2)$$

Where L is the number of compared time samples, which must be lower than the guard time. n is the index time sample.
Then,

$$Z = \sum_{n=0}^{l-1} S(n)\ exp(j2\pi\Delta fnTs)[S(n\ D)\ exp(j2\pi\Delta f(n\ D)Ts)]^{*} \qquad (3)$$

and

$$Z = exp(j2\pi\Delta fDTs) \sum_{n=0}^{l-1} |Sn|^{2} \qquad (4)$$

Then, the estimated frequency offset takes the form

$$\Delta f = -\frac{1}{2\pi DTs} angle(Z) \qquad (5)$$

The number of samples used for the estimation process is chosen to be less than half the guard band interval, starting from the beginning of its second quarter, to avoid the transient part affected by the channel. The complete guard band cannot be used because the errors in timing synchronization may lead to not exactly determine the start of the guard band. Taking more samples did not improve anything in the simulation results. The minimum number of correlation to give acceptable performance is determined. The limitation in this estimator is the angle (Z) which has the range from π to$-\pi$.

$$-\pi < angle(Z) < \pi; \qquad (6)$$

$$-\pi < 2\pi DTs\Delta f < \pi; \qquad (7)$$

$$\frac{-1}{2DTs} < \Delta f < \frac{1}{2DTs}; \qquad (8)$$

$$\frac{-fs}{2D} < \Delta f < \frac{fs}{2D}; \qquad (9)$$

$$\frac{-subcarrier\ spacing}{2} < \Delta f < \frac{subcarrier\ spacing}{2}; \qquad (10)$$

Where fs is the sampling frequency and D equals to the FFT size = 1024 samples. The limitation on the angle from $-\pi$ to π makes it impossible for the algorithm to estimate the coarse frequency offset which is multiple from the$\frac{fs}{D}$, which means it is multiples of $-\pi$ or π.

Another conclusion from the implementation point of view is that the use of this correlation based algorithm will allow a hardware reuse as it's the same correlation needed for symbol start algorithm. Also both fine frequency estimation and symbol start need the same basic operation, which is correlation [10]. To prepare the received preamble for correlation with stored preambles, the following steps are executed:

1) The channel effect on the received preamble must be reduced. This is done by multiplying each sample by the conjugate of its predecessor with 3 samples apart. For illustration, examine the following equation:

If $Q(k)$ is the received preamble in frequency domain, $G(k) = R\{Q(k)Q^{*}(k-1)\}$. This is on the assumption that the angles added by the channel on each 2 consecutive active subcarriers are nearly the same, then multiplying by the conjugate eliminate the channel's effect.

2) In case of using the second method hard decision is to be done to$G(k)$.

After estimating the fine frequency offset through the angle of maximum correlation - see equation (5) - compensating the offset is through multiplying the preamble samples by $exp(j2\pi\Delta fnTs)$ to correct the frequency offset.

However, there are some issues that should be noticed [11]:
(i) The efficiency of the estimator is directly proportional to the length of the repeated part.
(ii) The presence of multipath fading channel will significantly reduce the accuracy of the estimator. The presence of multipath will alter the cyclic prefix values of the preamble with respect to the corresponding values in the symbol. As a result, one would either consider a shorter duration of the preamble which will decrease the estimation accuracy or accept the distortion caused by the fading channel.
(iii) The phase rotation between the identical samples used to estimate the frequency offset should be in the range [$-\pi$, π), otherwise angle Z will fold by multiples of 2π and the estimate will be incorrect.

III. Joint Detection of Integral Carrier Frequency Offset And Cell Search

This algorithm considers joint detection of integral CFO and preamble index, under the assumption OFDM symbol boundaries and fine frequency offset have been acquired to reasonable accuracy. This assumption is valid with the timing and fine frequency offset simulation results. Based on an optimization formulation, a number of detection methods are driven of different complexity and optimization methods. The methods exploit the quasi-orthogonality among the OFDMA WiMAX preamble sequences as well as the organization of the nonzero subcarriers in the preambles [5]. Simulation results are presented to illustrate the performance of the methods, see section IV. This algorithm detect the integer frequency offset in range [-9 9 frequency offset pins] by the correlation in frequency domain between the received preamble -that is one of the 114 preambles- and the 114 preambles stored in the receiver. The max correlation indicates the most probable preamble sent, and then we can use it to calculate the integer frequency offset.

If the spacing of the nonzero subcarriers in the preamble is much smaller than the coherence bandwidth of the channel, then the channel responses at neighbouring preamble subcarriers are approximately equal, mathematically, this can be given by:

$$H(K+1) = H(K) + \Delta H(K) \qquad (11)$$

Where $|\Delta H(K)| \ll |H(K)|\, and\ K$ is an index for nonzero preamble subcarriers.
and,

$$R\{Q(k)Q^*(k\ -1)\} = R\{H(k)P_j(k\ +\ n)H^*(k\ -\ 1)P_j^*\ (k\ +\ n\ -\ 1)\} \approx |\Delta H(K)|^2 D_j(k+n) \qquad (12)$$

Where,
Q (k) is the received preamble in the frequency domain.
$P_j(k\ )$ is the stored preamble of index (j) in the frequency.
$D_j(k\ ) = P_j(k\ )\ \times\ P_j(k-1)$ Preamble (j) multiplied by a shifted version of one active subcarrier
n is the integral frequency offset normalized to the subcarrier spacing.

The normalized integral frequency offset means that multiplying each active subcarrier by the conjugate of its predecessor will cancel the channel-added phase and then we can correlate the preamble patterns shifted by the expected values of the integral carrier frequency offset and select the maximum correlation as follows:

$$M_n^{n,j} = \sum_{k=0}^{N_p-1} D_j(k+n) R\{Q(k)Q^*(k\ -1)\} \qquad (13)$$

Where $R\{Q(k)Q^*(k \square -1)\}$ is called the differential signal. The estimated integral CFO and preamble index are given by:

$$\widehat{(n,j)} = argmax_{n,j} M_{n,j}^n \qquad (14)$$

It should be noted that, the coarse frequency offset is usually estimated during the Cell-ID detection phase. Cell-ID detection is used to detect the preamble sequence being transmitted by the operating base station. Cell-ID detection is usually performed after fine frequency offset detection and correction. The Cell-ID detection block correlates the received frequency domain signal with the possible sequences. The correlators should take into consideration the possible shift, the range of which is determined by the allowed frequency offset defined in the standard. The Cell-ID detection block estimates the coarse frequency offset value and the detected preamble sequence [11].

IV. Algorithms Simulation Results

This section provides a detailed explanation and discussion of the simulation results of each algorithm. Those algorithms are simulated in ideal, AWGN, and dispersive fading channel with fixed point analysis. Each algorithm was simulated under fixed point analysis with the minimum number of bits achieved for each operation with acceptable performance. The parameters used for simulation are tabulated in Table 1.

A. *Cyclic-Prefix-Based Fine Frequency Offset Estimation*

To compute the percentage of errors the following conditions have been applied:

- Number of runs for x-axis = number of runs for y-axis =1000 runs.
- The area of consideration (-*fs* /2 to *fs* /2) is estimated 500 times for each dB, where *fs* is subcarrier spacing.
- The upper line at 2% represents the end range of error stated by the standard, for frequency offset error in estimation.

TABLE I
WiMAX OFDM Parameters

Symbol	Description	Relation	Used value
B	Nominal bandwidth	*B = 1/Ts*	0 MHz
L	Number of subcarriers	Size of *IFFT/FFT*	1024
G	Guard fraction	$\%\ of\ L\ for\ CP$	$1/4$
Fs	Sampling frequency	${}^{1}/_{Ts}$	11.2 MHz
Ts	Sample time	${}^{1}/_{Fs}$	89.2 nano sec
Ng	Guard band	$Ng\ =\ GL$	256
Tg	Guard time	$Tg\ =\ TsNg$	22.8 sec
T	OFDM symbol time	$T\ =\ Ts(L+Ng)$	114.2 sec
Bsc	Subcarrier spacing	$Bsc\ =\ B\ /\ L$	10.94 KHz.

As shown in Fig.4, Fig.5, Fig. 6 and Fig.7 the estimated error percentage is less than half of the maximum allowed error ,this means the cyclic prefix based fine frequency algorithm have acceptable performance in frequency offset estimation.

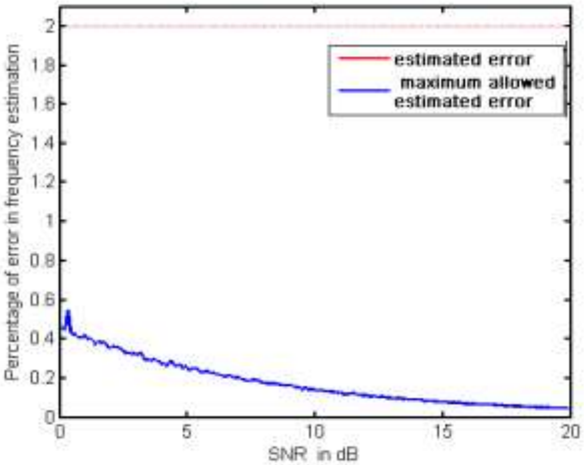


Fig. 4. Fine frequency offset estimation with different SNR under AWGN.

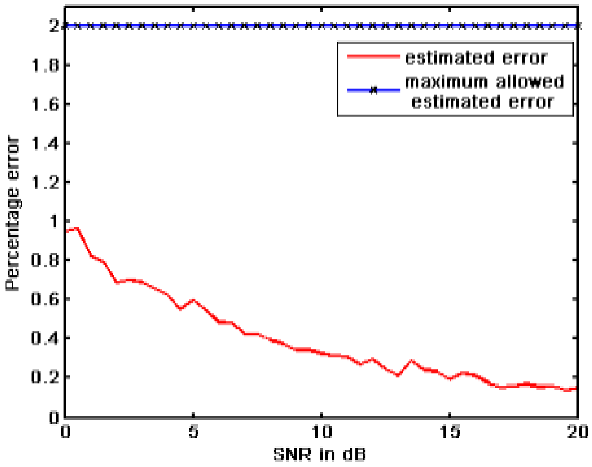


Fig. 5. Fine frequency offset estimation with different 16-bit fixed point analysis.

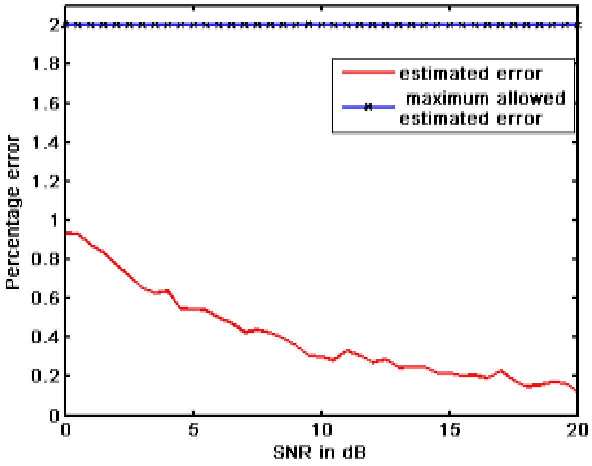


Fig. 6. Fine frequency offset estimation with different 18-bit fixed point analysis.

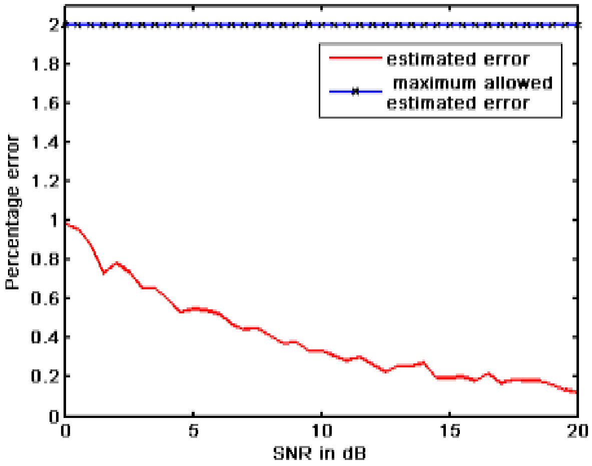


Fig. 7. Fine frequency offset estimation with different 20-bit fixed point analysis.

B. Joint-Based Coarse Frequency Offset Estimation

The following figures illustrate the performance of the coarse frequency offset algorithm through histograms under fading and AWGN. The conditions applied here are:

- Number of runs = 250 run.
- Number of integral carrier frequency offset tested = 6
- In these histograms, it’s taken into consideration to try preambles of different segments, to make sure it works for all 114 preamble patterns, thus different segments.

From the simulation result of joint based frequency coarse offset figures shown below, when the algorithm is applied under fading at 2 dB the estimated coarse frequency shift is equal to 6. This means that the algorithm was accurate at 246 runs; this is illustrated in Fig. 8 and Fig. 9. In Fig. 10 SNR was increased to 10 dB and the performance increased to 250 runs. Cell search results under fading at 2dB, 5 dB, and 10 dB are given in Fig. 11, Fig. 12, and Fig. 13 respectively. The preamble number is equal to 90 at both 246 and 250 runs.

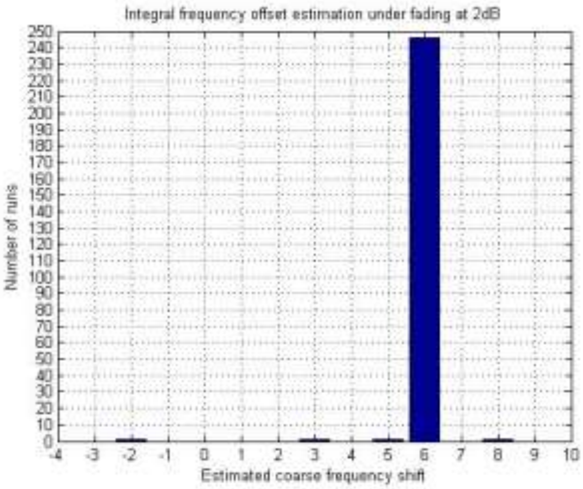


Fig. 8. Integral frequency offset estimation under fading at 2dB.

V. Conclusions

In OFDMA based mobile WiMAX, the receiver must align its carrier frequency as closely as possible to the transmitted carrier frequency. In this paper, the fine and coarse frequency offset estimation algorithms by using the packet preamble structure adopted by the IEEE 802.16 standardization workgroup have been presented and simulated. Joint detection of the coarse frequency offset and the cell search under fading and AWGN was obtained. The simulation results of these algorithms accurately estimated the frequency offset in the received frame. For future work, the whole transceiver system of the WiMAX can be simulated and implemented applying the same parameters. Also, the performance of these algorithms can be tested under different types of noise and channels.

ACKNOWLEDGMENT

Authors would like to thank the Department of Electronics Engineering, Faculty of Engineering, Sudan University of Science and Technology where this work has been carried.

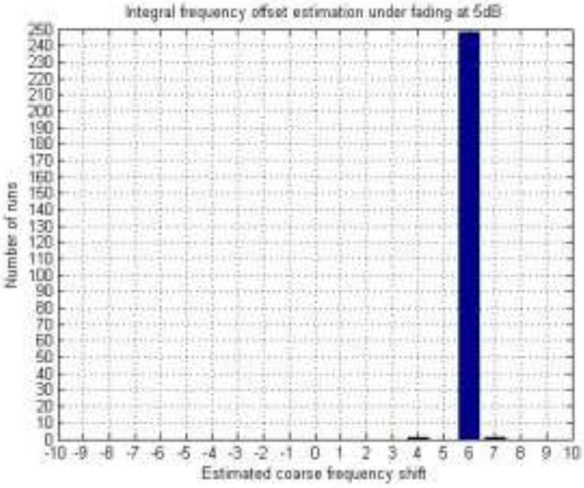


Fig. 9. Integral frequency offset estimation under fading at 5 dB.

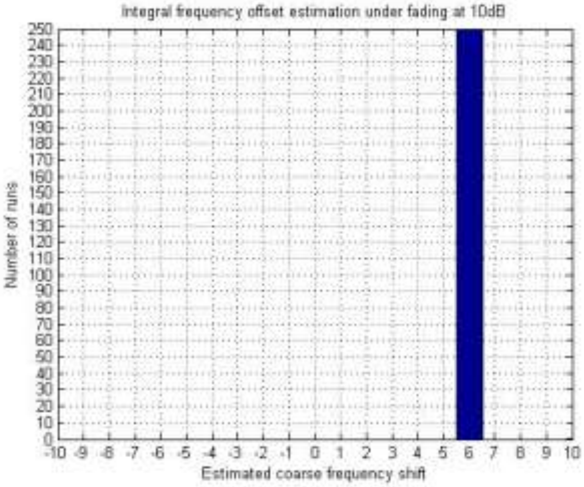


Fig. 10. Integral frequency offset estimation under fading at 10 dB.

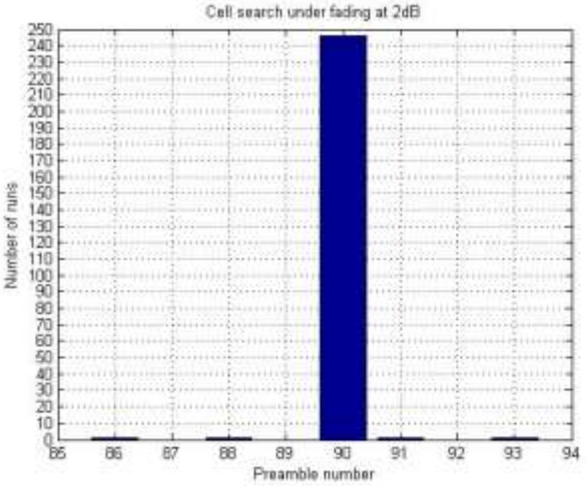


Fig. 11. Cell search results under fading at 2dB.

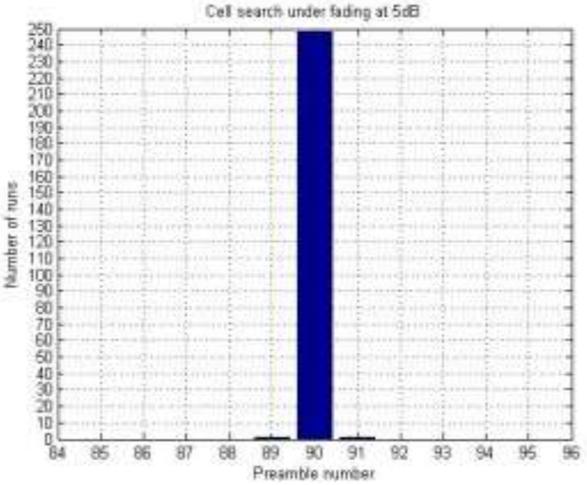


Fig. 12. Cell search results under fading at 5 dB.

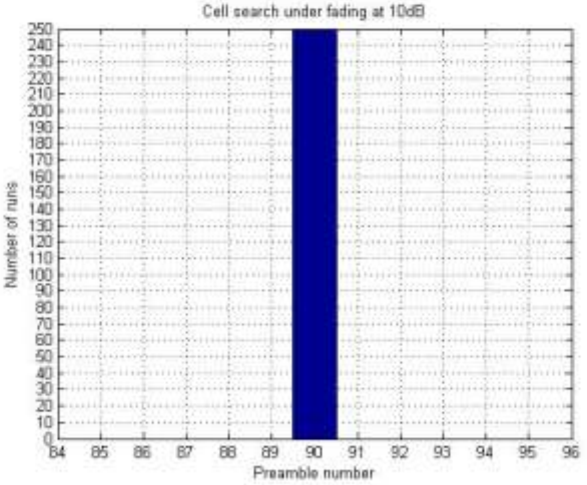


Fig. 13. Cell search results under fading at 10dB.

REFERENCES

[1] C. Ball, *LTE and WiMax Technology and Performance Comparison, Nokia Siemens Networks*, EW2007 Panel, 2007.

[2] B. Sidhu, H. Singh,, and A. Chhabra, *Emerging Wireless Standards WiFi, ZigBee and WiMax,* WASET.ORG, 2007.

[3] Jeffrey G. Andrews, Arunabha Ghosh, and Rias Muhamed, *Fundamentals of WiMAX: understanding broadband wireless networking*, Pearson Education. Inc, 2007.

[4] Juha Heiskala and John Terry, *OFDM wireless LANs A theoretical and practical Guide, Sams Publishing, 2002.*

[5] Kun-Chien Hung and David W. Lin,Joint "Detection of integral carrier frequency offset and preamble index in OFDMA WiMAX downlink synchronization" , *IEEE Proc, WCNC2007*.pp. 1959-1964.

[6] Kwang-Cheng Chen and J. Roberto B. de Marco, *Mobile WiMAX* , John Wiley & Sons. Ltd, 2008.

[7] kwang-cheng chen, *Introduction to Mobile Wimax*, Taiwan university, 2007.

[8] Loutfi Nuaymi, *WiMAX technology for broadband wireless access*, John Wiley and Sons Ltd, 2007.

[9] M. Morelli and M. Pun, "Synchronization Techniques For Orthogonal Frequency Division Multiple Access (OFDMA) A Tutorial Review", *Proc. IEEE*, July 2007, Vol. 95, no. 7. pp. 1394 – 1427, doi: 10.1109/JPROC.2007.897979.

[10] Mohamed Ismail Ali, "Simulation and implementation of the frequency synchronization and Viterbi decoding for the OFDMA-based Mobile WIMAX 802.16e", a thesis submitted to the Faculty of Engineering at Cairo University, 2007.

[11] Khairy, M. M., "A novel frequency offset estimation technique for Mobile WiMAX", Eur. Trans. Telecomm., 2011, Vol. 22. pp. 45–50. doi: 10.1002/ett.1462

Dr. Fakher Eldin Mohamed Suliman was born in Suda n in 1966.
He did his PhD, MSc, and BSc in 2004, 1999, and 1989 respectively, all in Electrical Engineering.
He is an assistant professor in the Electronics Engineer ing Department, College of Engineering,
Sudan University of Science and Technology (SUST) sin ce 2004.
He is the General manager of the Electronics System Research Center (ESRC) at SUST.
He is the coordinator of the postgraduate studies in his college.
He published a number of technical papers in international conferences and has two books under publication process.
His research interest includes; performance analysis and performance enhancement for Optical fiber systems, Wireless communications systems, and Switching systems.
Dr. Suliman is a Specialist Engineer in the Sudan Engineering Council and a Full Member of the Sudan Engineering Society.

Nuha M. Elhassan was born in Jeddah, Kingdom of Sau di Arabia, in 1988. She received the B.S. degrees in co mmunication engineering from SUST in 2009 .
From 2010 up to now, she is a Teaching Assistant in SU ST, University of Medical Science and Technology and Khartoum Collage of Technology.
Her Research Interest includes: performance analysis a nd performance enhancement for wireless Communications systems
Ms Elhassan is an Engineer in the Sudanese Engineering Council
Email: nohamohamed3@gmail.com
Tel: +249912493098

MS.Terteil Abdalla Abrahim was born in Sudan on De c,28, 1987
She did her Bsc. In 2009 in Electronics Engineering (Co mmunications), College of Engineering SUST
Since 2012 she is a Teaching Assistant in the School of Electronics, College of Engineering, SUST and
a part time teaching assistant at the Electrical and Elec tronic Department, College of Engineering,
International Of Africa University since 2013 until now.
She published two technical papers in international conferences.
Her Research Interest includes: performance analysis and performance enha ncement for the following:
Wireless Communications and Embedded Systems.
Ms.Terteil A. Abrahim is an Engineer in the Sudanese Engineering Council.
Email: terteil88@yahoo.com.
Tel: (+249) 922272954

Design and Performance Analysis of a newly designed 32-User Spectral Phase Encoding system operating at 2.5Gb/s for Fiber-Optic CDMA Networks

Savita R.Bhosale* Mr. S.B.Deosarkar **
Dr. BABASAHEB AMBEDKAR TECHNOLOGICAL UNIVERSITY, LONERE, TAL. - MANGAON,
DIST. - RAIGAD, PIN – 402103
Correspondence should be address to sr4bhosale@gmail.com and svt4bhosale@rediffmail.com

***Abstract* - Multiple access techniques are required to meet the demand for high-speed and large-capacity communications in optical networks, which allow multiple users to share the fiber bandwidth. Optical code-division multiple-access (O-CDMA) is receiving increased attention due to its potential applications for broadband access networks. We analyze a new technique for encoding and decoding of coherent ultra short light pulses. In particular, we discuss the temporal pseudo noise bursts generated by spectral phase coding of ultra short optical pulses.**

This paper describes a performance analysis of Spectral Phase Encoding optical code-division multiple-access scheme based on wavelength/time (W/T) codes and random phase codes. We have studied the optical simulator Encoding/Decoding at different fiber lengths & gain in terms of Quality factor (Q) and Bit Error Rate (BER) performance. We derive the bit error rate (BER) and QoS as a function of data rate, number of users, receiver threshold. We find that performance improves dramatically with optical power normalizer.Ultrashort light pulse CDMA could provide tens to hundreds of users with asynchronously multiplexed, random access to a common optical channel. The system supports 32 users while maintaining bit-error rate (BER) < 10^{-9} and required QoS for the correctly decoded signal at 2.5 Gbits/s bit rate.

Keywords : BER, ISD, MAI, NRZ, OCDMA, OOC, PSO, QoS, RZ.

I. INTRODUCTION

Due to economic advantages, maturing technology, and high information capacity, single-mode fiber- optic transmission media will be embedded in future telecommunications networks. A desirable feature for these future optical networks would be the ability to process information directly in the optical domain for purposes of multiplexing, demultiplexing, filtering, amplification, and correlation. Optical signal processing would be advantageous because potentially it can be much faster than electrical signal photon-electron-photon conversions. Several new classes of optical networks are now emerging [1]. For example, code-division multiple access (CDMA) networks using optical signal processing techniques were recently introduced [2]-[9].

CDMA is a type of spread spectrum communications [10] in which multiplexing is achieved by assigning different, minimally interfering code sequences to different user pairs. In fiber optic CDMA, users communicate by imprinting their message bits upon their own unique code, which they transmit asynchronously (with respect to the other transmitters) over a common channel. A matched filter at the receiver end ensures that data are detected only when they are imprinted on the proper code sequence (see Fig. 1). This approach to multiplexing allows transmission without delay and handles multi-access interference (contention) as an integral part of the multiplexing scheme.

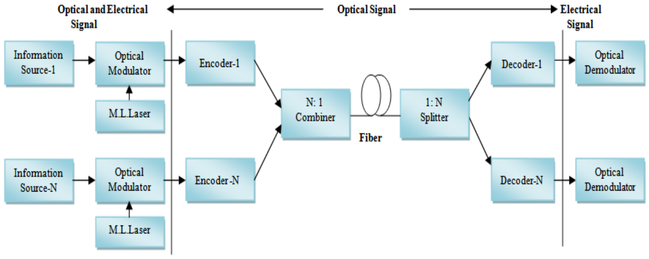


Fig. 1. Block diagram of Optical CDMA Network

In coherent OCDMA, encoding and decoding are performed either in time domain or in spectral domain based on the phase and amplitude of optical field . In coherent time spreading (TS) OCDMA, where the encoding/decoding is performed in time domain. In such a system, the encoding is to spread a short optical pulse in time with a phase shift pattern representing specific codes. The decoding is to perform the convolution to the incoming OOC using a decoder, which has an inverse phase shift pattern as the encoder and generates high level auto-correlation and low level cross correlations.

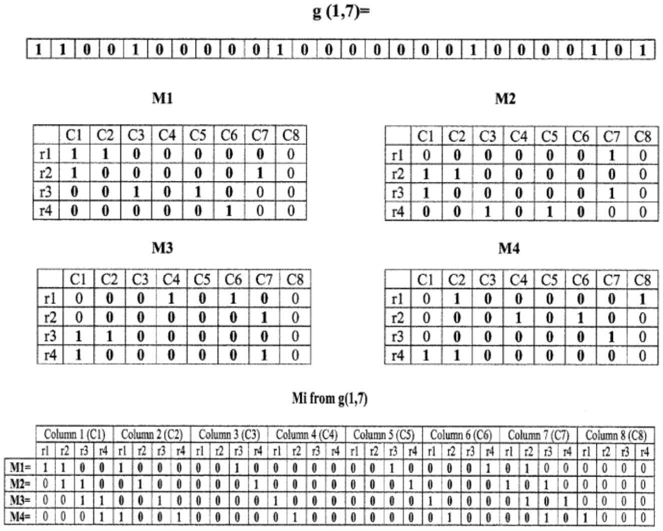
Manuscript received June 30, 2012.

Savita R. Bhosale is with Dr. Babasaheb Ambedkar Technological University, Lonere, Raigad. (MS) India Pin- 402103. M:9869579071,
Email: sr4bhosale@gmail.com , svt4bhosale@rediffmail.com

Dr. S. B. Deosarkar is with Dr. Babasaheb Ambedkar Technological University, Lonere, Raigad. (MS) India Pin- 402103

II. NUMERICAL SIMULATION

The encoders use delay line arrays providing delays in terms of integer multiples of chip times. The placement of delay line arrays and the amount of each delay and phase shifts are dictated by the specific of the signatures. PSO matrix codes are constructed using a spanning ruler or optimum Golomb ruler is a (0,1) pulse sequence where the distances between any of the pulses is a non repeating integer,hence the distances between nearest neighbors, next nearest neighbors, etc., can be depicted as a difference triangle with unique integer entries. The ruler-to-matrix transformation increases the cardinality (code set size) from one (1) to four(4) and the ISD (=Cardinality/CD)from 1/26 to 4/32=1/8. The ISD translates to bit/s/Hz when the codes are associated with a data rate and the code dimension is translated into the bandwidth expansion associated with the codes as follows:



g (1,7)=

1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1

M1

	C1	C2	C3	C4	C5	C6	C7	C8
r1	1	1	0	0	0	0	0	0
r2	1	0	0	0	0	0	1	0
r3	0	0	1	0	1	0	0	0
r4	0	0	0	0	0	1	0	0

M2

	C1	C2	C3	C4	C5	C6	C7	C8
r1	0	0	0	0	0	0	1	0
r2	1	1	0	0	0	0	0	0
r3	1	0	0	0	0	0	1	0
r4	0	0	1	0	1	0	0	0

M3

	C1	C2	C3	C4	C5	C6	C7	C8
r1	0	0	0	1	0	1	0	0
r2	0	0	0	0	0	0	1	0
r3	1	1	0	0	0	0	0	0
r4	1	0	0	0	0	0	1	0

M4

	C1	C2	C3	C4	C5	C6	C7	C8
r1	0	1	0	0	0	0	0	1
r2	0	0	0	1	0	1	0	0
r3	0	0	0	0	0	0	1	0
r4	1	1	0	0	0	0	0	0

Mi from g(1,7)

	Column 1 (C1)				Column 2 (C2)				Column 3 (C3)				Column 4 (C4)				Column 5 (C5)				Column 6 (C6)				Column 7 (C7)				Column 8 (C8)			
	r1	r2	r3	r4	r1	r2	r3	r4	r1	r2	r3	r4	r1	r2	r3	r4	r1	r2	r3	r4	r1	r2	r3	r4	r1	r2	r3	r4	r1	r2	r3	r4
M1=	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0
M2=	0	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0	0	0
M3=	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0	0
M4=	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0

Fig. 2. Constructing the four pseudo orthogonal (PSO) matricesM1. . .M4 from the single optimum Golomb ruler g(1,7).

$$\mathrm{ISD}\ = \frac{(\text{throughput})}{(\text{bandwidth required})}$$

$$= \frac{(\text{cardinality} \times \text{data rate})}{\left(\frac{1}{\mathrm{Tb}}\right)(\text{bandwidth expansion})}$$

$$= \frac{(\mathrm{n} \times \mathrm{r} \times \mathrm{R})}{(\mathrm{R})(\mathrm{CD})}$$

$$= \frac{\mathrm{n} \times \mathrm{r}}{(\mathrm{CD})}$$

The enhanced cardinality and ISD, while preserving the OOC property, are general results of the ruler-to-matrix transformation. We can convert the PSO matrices to wavelength/time (W/T) codes by associating the rows of the PSO matrices with wavelength (or frequency) and the columns with time-slots, as shown in Table I. The matricesM1….M32 are numbered 1…32 in the table, with the corresponding assignment of wavelengths and time-slots. For example, code M1 is (λ1 ; λ1 ; λ3; λ1) and M9 is (λ1,λ4;0;λ7,λ8;0); here the semicolons separate the timeslots in the code. (The codes M1 and M9 are shown in bold numerals.)We focus on codes like M1 because it shows extensive wavelength reuse, and on codes likeM9 because it shows extensive time-slot reuse. It is the extensive wavelength and time-slot reuse that gives these matrix codes their high cardinality and high potential ISD.

Four mode-locked lasers are used to create a dense WDM multi-frequency light source. Pseudo-orthogonal (PSO) matrix codes [3] are popular for OCDMA applications primarily because they retain the correlation advantages of PSO linear sequences while reducing the need for bandwidth expansion. PSO matrix codes also generate a larger code set. An interesting variation is described in [1] where some of the wavelength/time (W/T) matrix codes can permit extensive wavelength reuse and some can allow extensive time-slot reuse. In this example, extensive time-slot reuse sequence is used. There are four time slots used without any guard-band giving the chip, period of 100 ps. Code1,code 5,code3 and code9 codes are used for time spreading. Code set to apply binary phase shift mapped as M1:{1;0;1;0;1;1;1;1} M2:{1;0;1;1;1;1;1;1}………………… M32:{0;0;1;1;1;1;1;0} (1 represents as a π phase shift, 0 represents as no phase shift)

TABLE I
THE 32 PSO MATRIX CODES INTERPRETED AS W/T MATRIX CODES

Wavelengths (W)	Time slots (S)			
	1	2	3	4
λ1	1,9, 17,25	1,14, 29	19,24, 26	1,7,10, 11,20,32
λ2	2,10, 18,26	2,15, 17,30	20,25, 27	2,8,11, 12,21
λ3	3,11, 19,27	3,16, 18,31	1,21, 26,28	3,12, 13,22
λ4	4,9,12, 20,28	4,19, 32	2,22, 27,29	4,13, 14,23
λ5	5,10,13, 21,25,29	5,20	3,23, 28,30	5,14, 15,24
λ6	6,11,14, 22,26,30	6,21	4,17,24, 29,31	6,15, 16
λ7	7,12,15, 23,27,31	7,17, 22	5,9,18, 30,32	7,16
λ8	8,13,16, 24,28,32	8,18, 23,25	6,9,10, 19,31	8

TABLE II
SPE O-CDMA SYSTEM PARAMETERS USED FOR SIMULATION

Parameter	Value
Code length	8
Channel spacing	0.4 nm
Wavelength	4 at 1550,1550.4,1550.8,1551.2 nm
Chip time	4
Chip rate	1.25E-10
Bit rate	2.5 Gbits /s
Modulation Format	NRZ and RZ
Fiber length	60 to 180 km
Measurements	Eye diagram, Bit error rate and Quality factor

III. PROPOSED SCHEME SPE O-CDMA

1) Lasers (mode locked laser)2) Encoders 3) Multiplexers 4) Optical fiber of 60 to 180 km length 5) De multiplexers 6) Decoders 7) Receiver 8)BER analyzer 9) Eye Diagram analyzer 10) Signal analyzer The simulation setup for Spectral Phase Encoding Optical CDMA is shown in figure 3. The MLL is used to generate four wavelengths, range from1550 nm to 1551.2 nm, with 0.4nm wavelength spacing, this carrier signal is used to modulate the pseudo random bit sequence (PRBS) data of the user. An intensity modulator which is External Modulator uses on-off keying modulation to modulate the multiplexed 4 wavelengths according to the NRZ and RZ electrical data. For analysis, Eye Diagram analyzer, Beat Error tester and Signal analyzer is used.

IV. SIMULATION OF SPE O-CDMA SYSTEM ONE USER

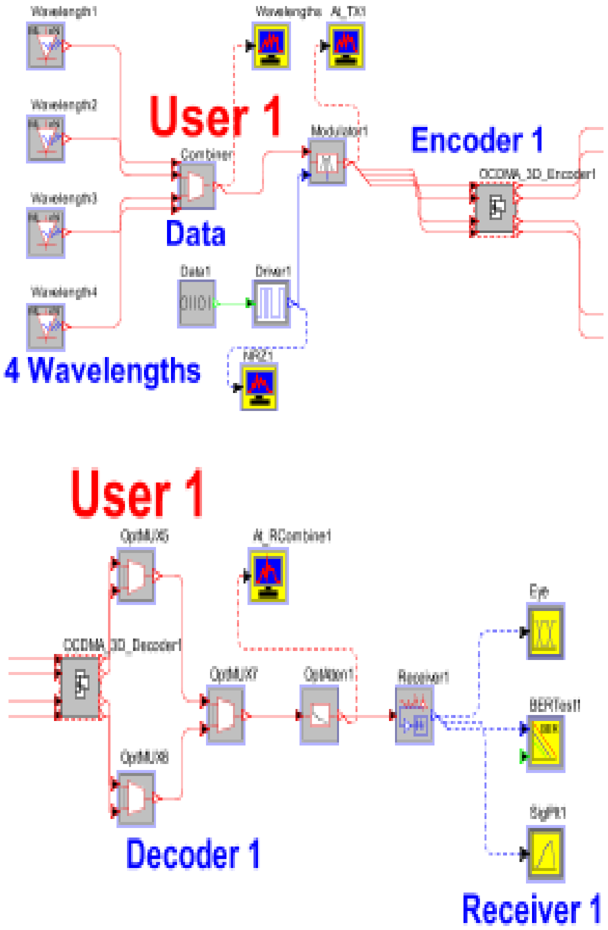


Fig. 3. Simulation setup for SPE O-CDMA Transmitter and Receiver of User1

Figure 4 shows dense wavelength spectrum for four wavelengths respective encoders, which have been assigned a unique W/T code respective to each encoder.

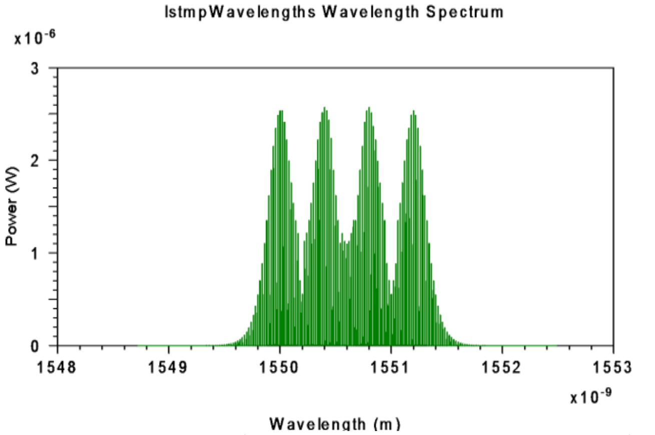


Fig. 4. Wavelength Spectrum for Spectral Phase Encoding Optical CDMA for 32 Users

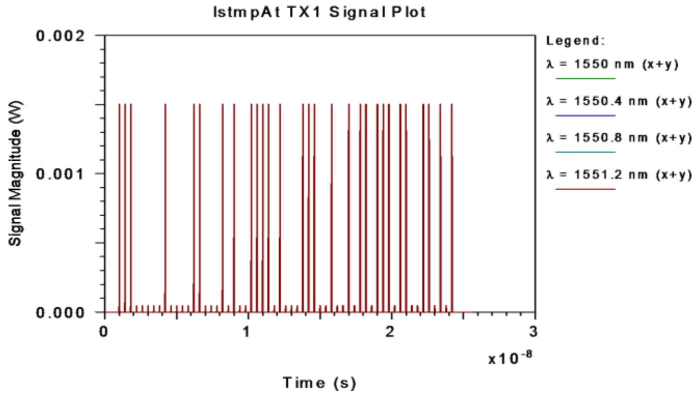


Fig. 5. Modulated data before encoder of User 1

Figure 5 shows modulated data before encoding.

The encoded data from all users are multiplexed by Optical MUX and then passed through a 60 km and 180 km span of standard single mode optical fiber followed by a loss compensating optical amplifier which is Opt Amp. The output signal from a fiber span is then passed through OptSplit1 to split the signal and routed to the user's decoder. The decoder uses optical filters and inverse delay line arrays providing delays in terms of integer multiples of chip times and phase shift pattern. The decoded signal finally arrives at optical receiver (Receiver), BER Test and Eye Diagram. Eye diagram analyzer has been used to take the plot of Eye pattern at the receiver end. Bit error rate values for different number of transmitting users have been taken from BER Tester.

The system has been redesigned for different number of users. In spite of the use of orthogonal codes, the main effect limiting the effective signal-to-noise ratio of the overall system is the interference resulting from the other users transmitting at the same time, which is called Multiple Access Interference (MAI). MAI is the major source of noise in OCDMA systems. System performance is tested at 2.5 Gbits/s bit rate, NRZ and RZ data modulation format, BER and quality factor at different data modulation format noted. Eye diagram observed at different fiber length.

V. Performance Analysis

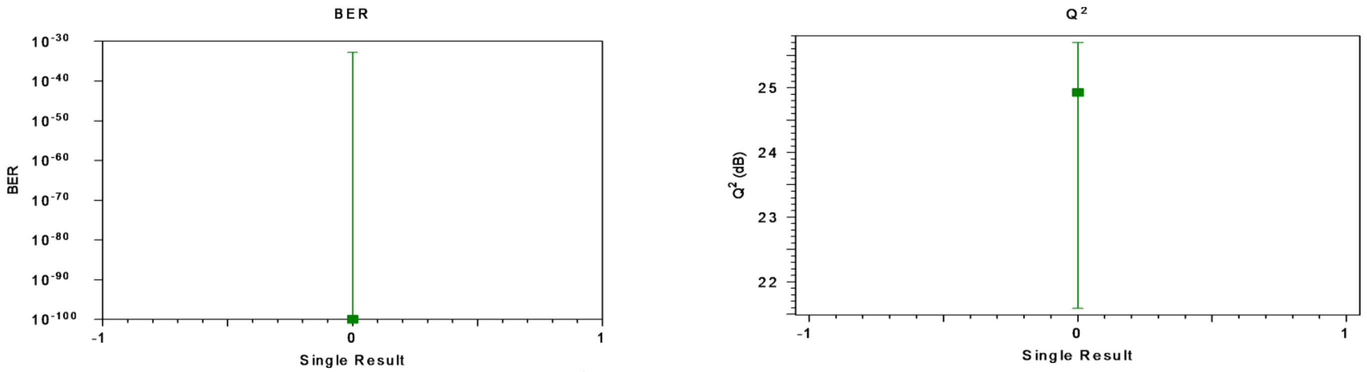


Fig. 6. BER and Quality factor at User1 using Optical Power Normalizer

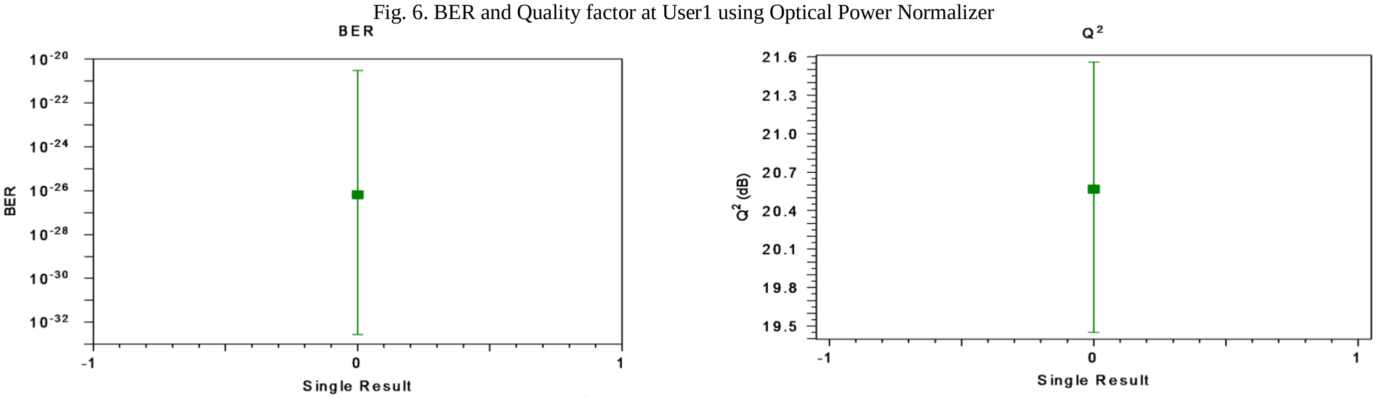


Fig. 7. BER and Quality factor at User16 using Optical Power Normalizer

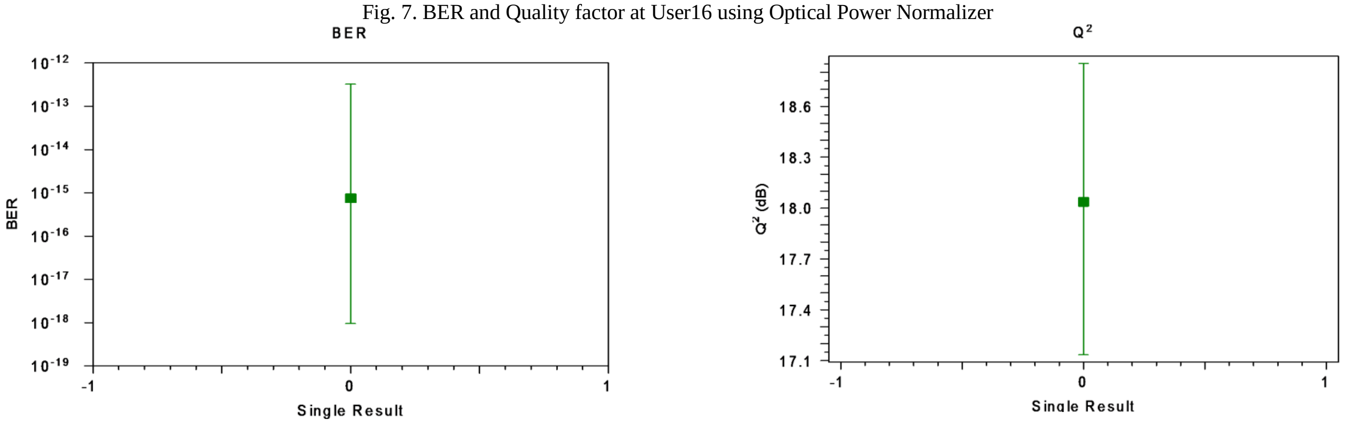


Fig. 8. BER and Quality factor at User32 using Optical Power Normalizer

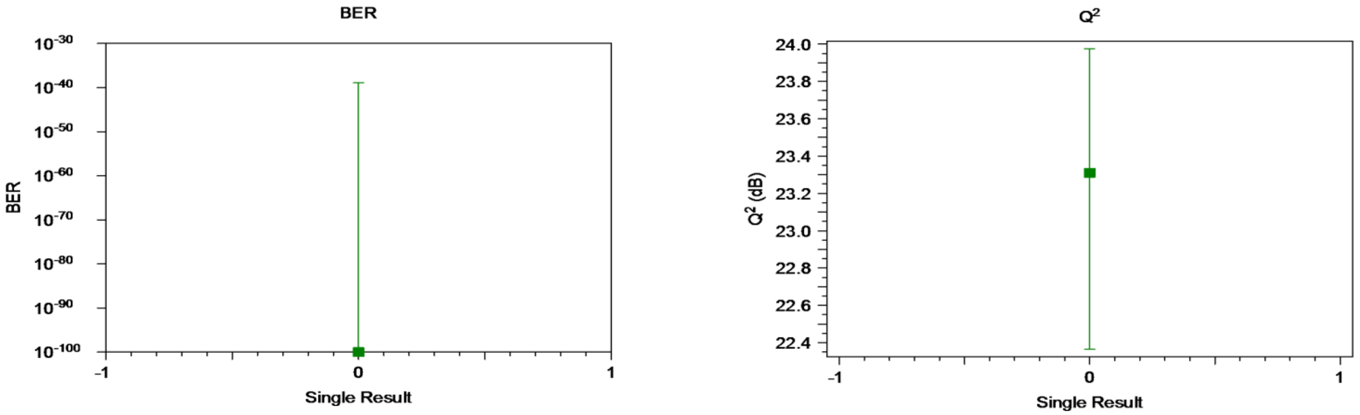


Fig. 9. BER and Quality factor at User1 using Optical Attenuator

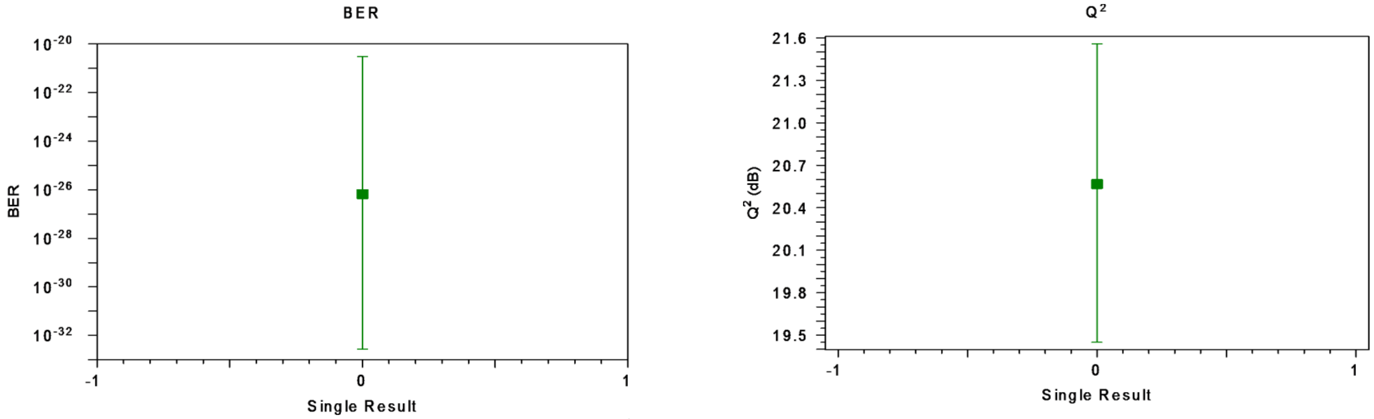


Fig. 10. BER and Quality factor at User16 using Optical Attenuator

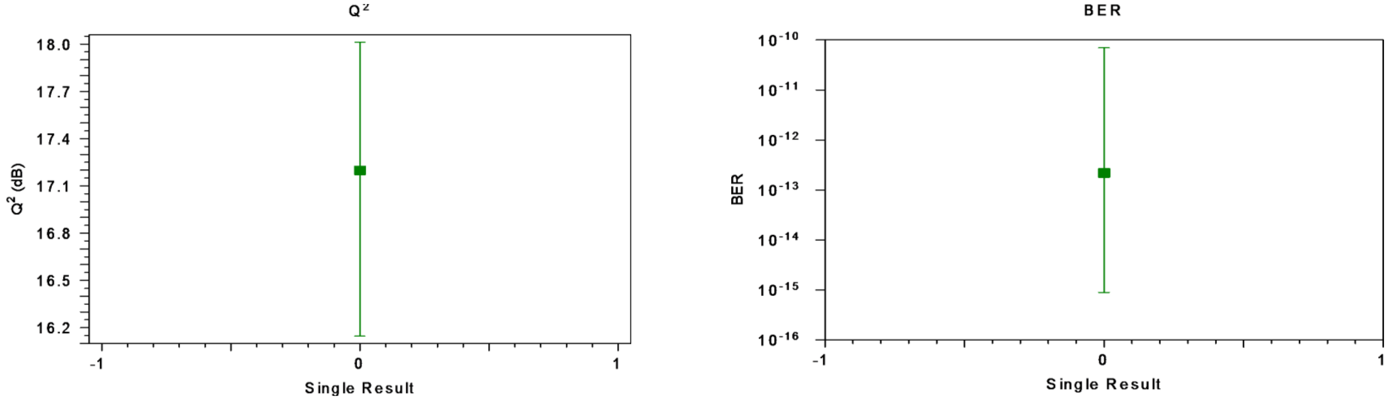


Fig. 11. BER and Quality factor at User32 using Optical Attenuator

Figure 6,7, 8, 9,10 and 11 shows BER and Quality factor of SPE O-OCDMA system using optical attenuator and optical power normalizer at User1,User8,User16 and User32 respectively. As active number of users increases system performance degrades. System performance is analyzed at 2.5 Gb/s bit rate, -20 dB received power and 60km to 180 km fiber span. System performance is extremely good by using optical power normalizer. Spectral phase encoding O-CDMA system using optical attenuator and optical power normalizer system supports 32 users at 2.5Gb/s and offer s low Bit Error Rate and good quality of service.

Figure 12 and 13 shows System performance degrades as fiber length increases .The SPE O-CDMA system offers High Quality factor and extremely less BER at -20 dBm received power and over 60km to 180 km fiber length.

Eye opening is good using optical power normalizer as compare to optical attenuator. Eye diagram analysis is carried out at 60 km fiber span and at 180 km fiber span.SPE OCDMA system using optical power normalizer performance is good as compare to optical attenuator over 60km and180 km fiber span.

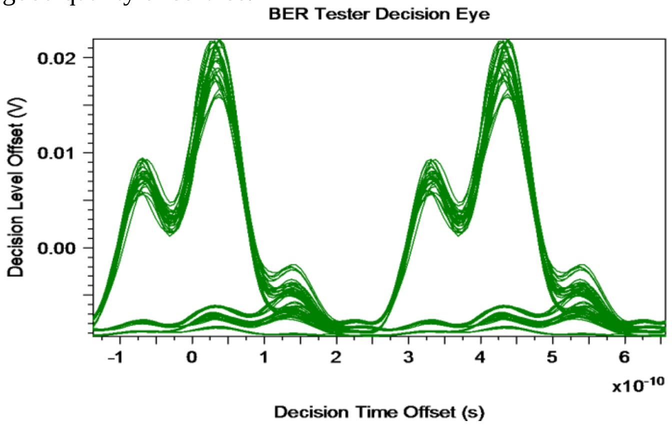


Fig. 12. Eye Diagram analysis at User32 using Optical Power Normalizer over 60 km fiber span

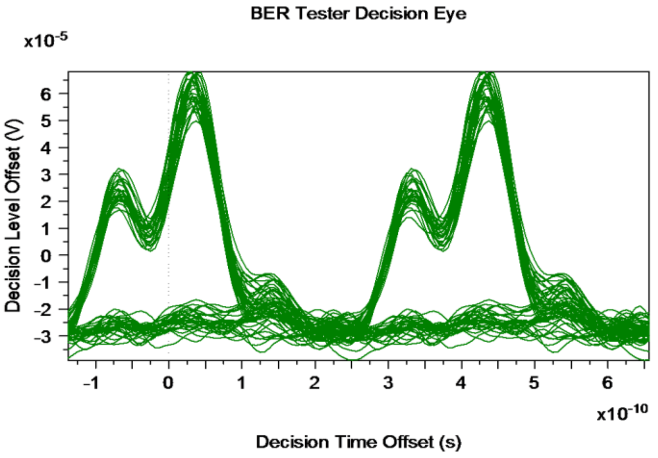


Fig.13. Eye Diagram analysis at User32 using Optical Power Normaliszr over180 km fiber span

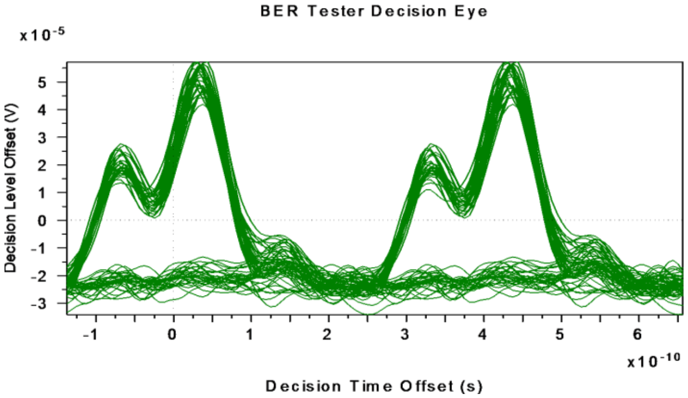


Fig. 14. Eye Diagram analysis at User32 using Optical Attenuator over 60 km fiber span

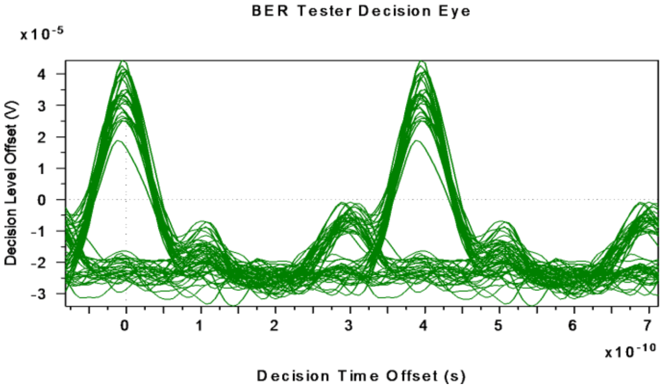


Fig. 15. Eye Diagram analysis at User32 using Optical Attenuator over 180 km fiber span

Figure 12,13,14 and 15 shows System performance degrades as fiber length increases .The SPE O-CDMA system offers high Quality factor and extremely less BER at -20 dBm received power and over 60 km to 180 km fiber length using optical power normalizer.

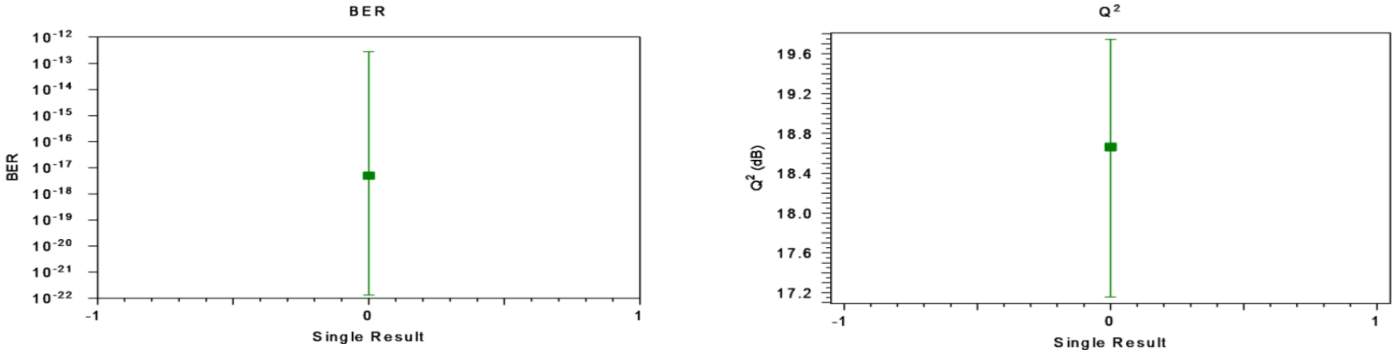


Fig. 16. BER and Quality factor at User1 using Optical Attenuator for RZ data modulation format

Figure 16, 17 and 18 shows SPE O-CDMA system performance of RZ data modulation format, Results indicates enhancement in BER and quality factor for NRZ data modulation format as compared to RZ data modulation.

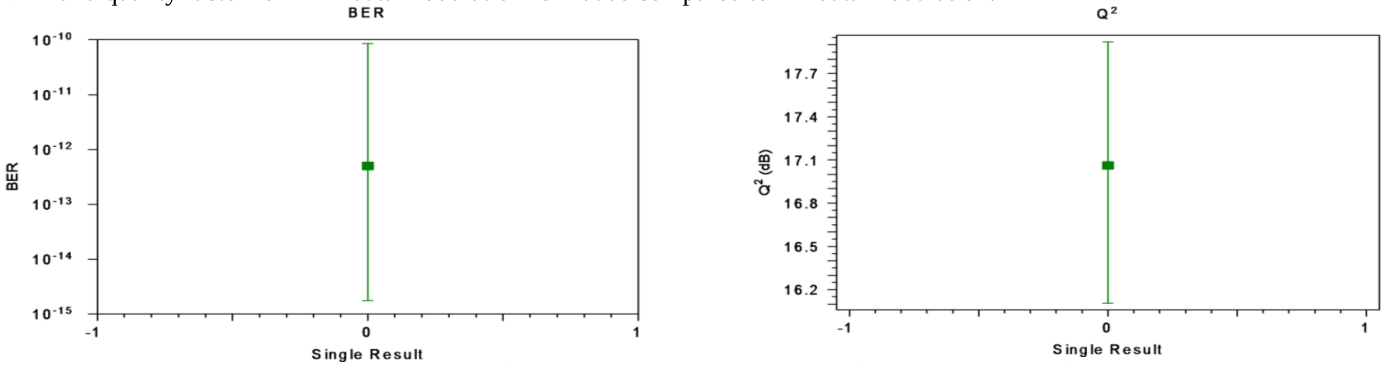


Fig. 17. BER and Quality factor at User16 using Optical Attenuator for RZ data modulation format

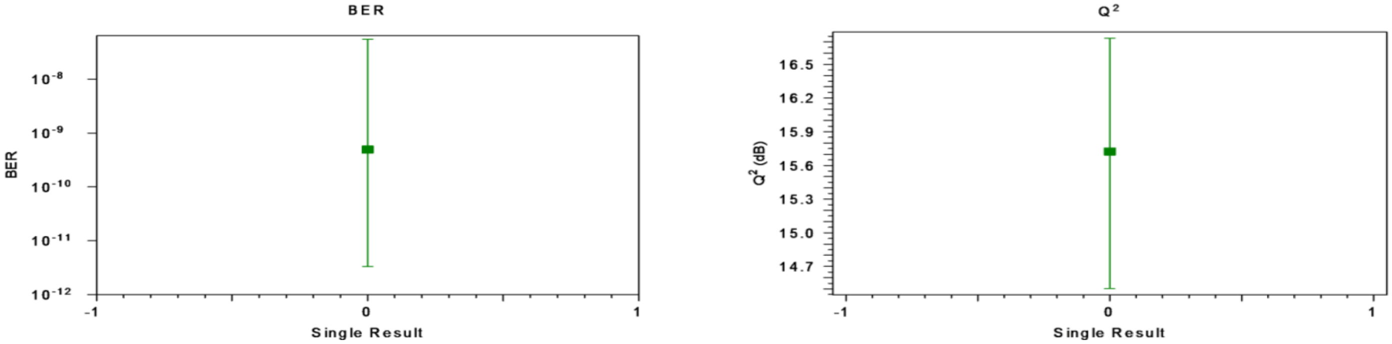


Fig. 18. BER and Quality factor at User 32 using Optical Attenuator for RZ data modulation format

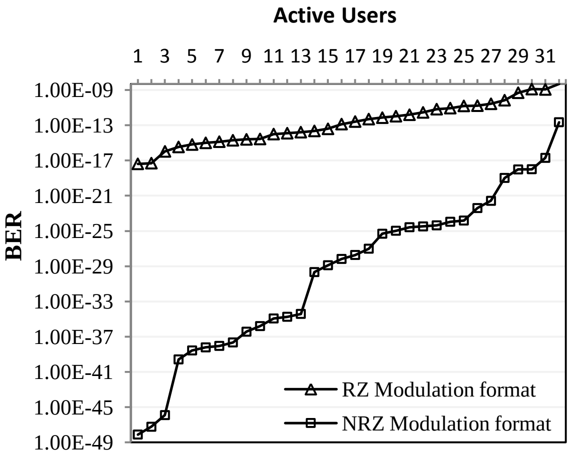


Fig. 19. System performance for RZ and NRZ data modulation format for 32Users

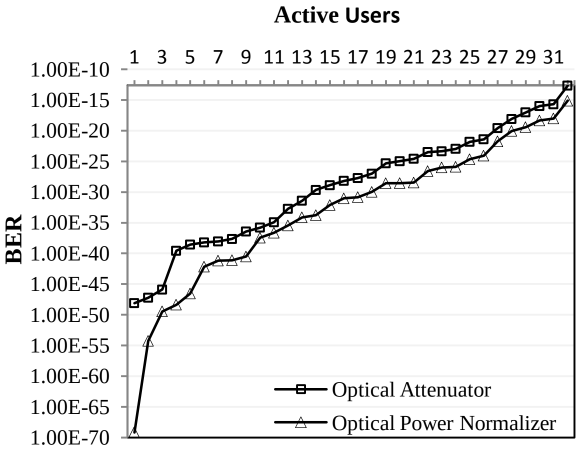


Fig. 20. System performance using Optical Power Normalizer and Optical Attenuator in terms of Quality factor for 32 Users

Figure 19 and 20 represents graphical representation of Beat Error rate and Quality factor of SPE O-CDMA system .System performance is analyzed for NRZ and RZ data modulation format and using optical attenuator and optical power normalizer for 32 numbers of active users. Results indicates enhancement in BER and quality factor for NRZ data modulation format as compared to RZ data modulation format, low BER and high Quality of service using optical power normalizer.Beat Error Rate of SPE OCDMA system using Optical Power Normalizer at User1 and User32 is 1.00E-70 and 1.00E-16 respectively, while SPE OCDMA system using Optical Attenuator at User1 and User32 is 1.00E-49 and 1.00E-13 respectively, for NRZ and RZ data modulation format BER for NRZ is at User1 and User32 is 1.00E-49 and 1.00E-13 respectively, for RZ format at User1 and User32 is 1.00E-17 and 1.00E-09 respectively.

V. CONCLUSION

The multiple access interference effect was also seen at the optical receiver end in optical CDMA which degraded the efficiency of system by increasing bit error rate. Use of spectral phase encoding O-CDMA system reduced the MAI as seen in the bit error rate performance and quality factor. The spectral phase encoding O-CDMA system performance is good for 32 users at 2.5Gbits/s bit rate using optical power normalizer. The performance of SPE O-CDMA system is analyzed by using NRZ and RZ data modulation format, while NRZ data modulation format offers extremely good performance than RZ data modulation format. The SPE O-CDMA system has been successfully demonstrated at system capacity of 80 Gbits/s over 180 km of fiber length. This newly designed SPE O-CDMA offers high Quality factor and less Beat Error Rate <10^{-9} .Moreover these results are more realistic as practical impairments have been considered with -15 dB and -20 dBm received power for optical attenuator, optical power normalize respectively and for permissible BER of 10^{-9}.

REFERENCES

[1] X. Wang and K. Kitayama, “Analysis of beat noise in coherent and incoherent time-preading OCDMA,” J.Lightwave Technol 22, 2226-2235, (2004).

[2] T. H. Shake, “Confident performance of –encoded optical CDMA”, J. Lightwave Technol.23, 1652– 1663, (2005).

[3] AntonioMendez Senior Member, IEEE, Robert M. Gagliardi,Fellow, IEEE, Vincent J.Hernandez J.“Design and performance analysis of Wavelength/Time (W/T) matrix codes for optical CDMA”. Journal of lightwave technology Vol.21November 2003.

[4] D. E. Leaird, Z Jiang, and A. M. Weiner,“Experimental investigation of security issues inOCDMA: a code-switching scheme”, Electron. Lett.41, 817-819, (2005).

[5] X. Wang, N. Wada, T. Miyazaki, and K. Kitayama,“Coherent OCDMA system using DPSK data format with balanced detection”, IEEE Photonic Technol.Lett. 18, 826-828, (2006).

[6] Stock and E. H. Sargent, “The role of optical CDMA in access networks”, IEEE Communication Magazine40, 83- 87 (2002).

[7] Z. Gao, X Wang, N. Kataoka and N. Wada,“Demonstration of time-domain spectral phase encoding/DPSK data modulation using single phase modulator”, presented in LEOS Summer Topical 2009, New port, CA, USA, 2009.

[8] Z. Jiang, D. Seo, S. Yang, D. E. Leaird, R. V.Roussev, C. Langrock, M. M. Fejer, and A. M.Weiner, “Four-user 10-Gb/s spectrally phase-codedO-CDMA system operating at ~ 30 fJ/bit” IEEEPhotonics Technol. Lett., 17, 705-707, (2005).

[9] Xu Wang and Naoya Wada “Reconfigurable Time Domain Spectral Phase Encoding/Decoding Scheme Using Fibre Bragg Gratings for Two-dimensional Coherent OCDMA”, ECOC’08, P.3.11, September Brussels, Belgium, 2008.

[10] Xu Wang and Naoya Wada, "Spectral phase encoding of ultra-short optical pulse in time Domain for OCDMA application", Optics Express15(12):7319-7326 (2007).

[11] Stok and E. H. Sargent, “The role of optical CDMAin access networks,” IEEE Commun. Mag., vol. 40,no. 9, pp. 83–87, Sep. 2002.

[12] Jawad A. Salehi “Emerging Optical CDMA Techniques and Application” International Journal of Optics and Photonics,Voll.No.1,June2007.

[13] A. J. Mendez, R. M. Gagliardi, V. J. Hernandez, C.V. Bennet and W. J. Lennon, “High-Performance optical CDMA system based on 2-D optical orthogonal codes,” IEEE Journal of Lightwave Technology, vol. 22, pp. 2409-2419, Nov. 2004.

[14] Z. Jiang, D. S. Seo, S.-D. Yang, D. E. Leaird, A. M.Weiner, R. V. Roussev, C. Langrock, and M. M.Fejer, “Four user, 2.5 Gb/s, spectrally coded OCDMA system demonstration using low power nonlinear processing,” in Optical Fiber Communication Conference, 2004Technical Digest Series (Optical Society of America, 2004), paper PDP29.

[15] Ryan P. Scott, Wei Cong, Vincent J. Hernandez,Kebin Li, Brian H. Kolner,Jonathan P. Heritage, and S. J. Ben Yoo, “An Eight-User Time-Slotted SPECTS O-CDMA Testbed: emonstration and Simulations,” , Journal of Lightwave Technology VOL. 23, NO. 10 “High-Performance optical CDMA system based on 2-D optical orthogonal codes,” IEEE Journal of Lightwave Technology, vol. 22, pp. 2409-2419, Nov. 2004.

[14] Z. Jiang, D. S. Seo, S.-D. Yang, D. E. Leaird, A. M.Weiner, R. V. Roussev, C. Langrock, and M. M.Fejer, “Four user, 2.5 Gb/s, spectrally coded OCDMA system demonstration using low power nonlinear processing,” in Optical Fiber Communication Conference, 2004Technical Digest Series (Optical Society of America, 2004), paper PDP29.

[15] Ryan P. Scott, Wei Cong, Vincent J. Hernandez,Kebin Li, Brian H. Kolner,Jonathan P. Heritage, and S. J. Ben Yoo, “An Eight-User Time-Slotted SPECTS O-CDMA Testbed: emonstration and Simulations,” , Journal of Lightwave Technology VOL. 23, NO. 10 OCTOBER 2005.

Savita R.Bhosale Research Scholar Dr.Babasaheb Ambedkar Technological University Lonere (MS) ,India.Savita R.Bhosale received the B.E. degree in electronics and Telecommunication engineering from Dr.Babasaheb Ambedkar Maratwada University, India in 1993, and finished the M.Tech. degree course in electronics and Telecommunication

Engineering from Dr.Babasaheb Ambedkar Technological University Lonere (MS), India in 2006. Since 1998, She was worked as Lecturer and from 2006 working as Assistant Professor till date in MGM’s college of Engineering and Technology, India. Her research interests include Telecommunication and, optical fiber communication, optical networking, wireless and mobile communication.

Shankar B. Deosarkar

Shankar B. Deosarkar Received his graduate degree in electronics engineering in the year 1988 from Amravati University, his M.Tech and Doctorate degree in the area of Microwave Communication in the year 1990 and 2004 respectively from S.G.G.S. Institute of Engineering and Technology, Nanded.

At present he is guiding three Research Scholars in the area of EMI / EMC and Microstrip Antenna Design. Presented his research contribution at IEEE International Conferences at IIT’S, USA, UK, CANADA, ITALY and SINGAPOORE.He had delivered invited talks at McGill University, Montreal, Canada, Electromagnetic Research Center Ottawa, Government of Canada and Princeton University, New Jersey, USA and UGC / AICTE refresher courses. He is also been member of the programme committee at the various international conferences and reviewer of few books of McGraw Hill and PHI publications in the area of Microwave Communication as well reviewer of several national and international IEEE Conferences in the area of Microwave Communication,optical fiber communication.

Volume 1 Issue 1, Jul 2012, ISSN: 2288-0003

ICACT-TACT
JOURNAL

GIRI Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 463-824
Business Licence Number : 220-82-07506, Contact: secretariat@icact.org Tel: +82-70-4146-4991