JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

It can be observed that the Internet traffic generated by multiplayer computer games, radio broadcasts, music files, videos, etc., is rapidly increasing. No doubt, the future Internet will carry more and more traffic related to different multimedia applications. It is also envisaged that future "in home" networks will be also mostly used for such purposes. Even the 3G mobile telephony is being marketed as a vehicle for watching television programs while on the move. The similar trend can be observed in most of the current research in the area of communication systems and networks, i.e., the envisaged application are high volumes of data generated by multimedia applications delivered with the certain level of the quality of service (QoS) to mobile customers.

This special issue on the multimedia communications contains selected papers from the 3rd Workshop on the Internet, Telecommunications and Signal Processing, WITSP'2005, which was held in December 2004 in Adelaide, South Australia. The Workshop built on the successes of two previous events, WITSP'2002 – held in Wollongong in 2002, and WITSP'2003 – held in Coolangatta on the Gold Coast in 2003. The response to the original call for papers has exceeded our expectations, with 165 submissions, which have been 12 more than for the previous workshop combined with the 7th International Symposium on DSP and Communication Systems and almost three times that of the 1st WITSP held in Wollongong. All submitted papers have been peer reviewed, and each paper received two independent reviews. Based on those reviews, 82 papers have been accepted and finally 76 papers included in the workshop program. After the Workshop, the authors of 11 papers were asked to revise and extend their contributions to form this special issue.

The papers invited to this issue cover a range of topics spanning from the image coding, unequal error protection coding and data encryption, through the problems of mobile ad hoc networks, traffic management in the high speed Internet, to techniques enabling better bandwidth utilization and accuracy of hardware involved in signal estimation at the receiver in the presence of high level of noise. The papers are presented in the order resembling the IP protocol stack.

The first group of four papers deals with the issues related directly to multimedia applications. The paper *Gaze-J2K: gaze-influenced image coding using eye trackers and JPEG 2000* by A. Nguyen, V. Chandran, and S. Sridharan presents a system incorporating the use of eye tracking and JPEG 2000 to allow a customized encoding of an image by using the user's gaze pattern. It is followed by the paper *Benchmarking image codecs by assessment of coded test images: the development of test images and new objective quality metrics* by A. Punchihewa, D. G. Bailey, and R. M. Hodgson describing a simple but accurate method for fast assessment of the degree of blockiness, edge-blur and ringing due to image compression. The efficiency of the method is demonstrated for a JPEG codec at different compression levels. The third paper *Application of convolutional interleavers in turbo codes with unequal error protection* by S. Vafi, and T. A. Wysocki demonstrates usefulness of convolutional interleavers to design unequal error protection turbo codes. By using such codes, different parts of multimedia data blocks can be differently protected significantly decreasing the total code redundancy compared to the case where the whole data block were protected at the level required for the most important part of the block. The last paper in the group *An identity-based broadcast encryption scheme for mobile ad hoc networks* by C. Y. Ng, Y. Mu, and W. Susilo proposes a secure protocol for mobile devices to construct a group key for a set up of a secure dynamic communication network.

The fifth paper of the issue *An adaptive LQG TCP congestion controller for the Internet* by L. B. White and B. A. Chiera addresses the problem of congestion control for transmission control protocol (TCP) traffic in the Internet. The proposed method is based on an adaptive linear quadratic gaussian (LQG) formulation that uses an extended least squares system identification algorithm combined with optimal LQG control.

The next two papers: *Load-balanced route discovery for mobile ad hoc networks* by M. Abolhasan, J. Lipman, and T. A. Wysocki, and *Effect of unequal power allocation in turbo coded multi-route multi-hop networks* by T. Wada, A. Jamalipour, K. Ohuchi, H. Okada, and M. Saito, deal with the important type of the networks which will be also carrying a significant proportion of multimedia traffic in the future. Such networks are promising candidates for next generation mobile communications and will facilitate extending the coverage area without the significant infrastructure costs.

The following three papers: *An adaptive iterative receiver for space-time coding MIMO systems* by C. Teekapakvisit, V. D. Pham, and B. Vucetic, *Exact pairwise error probability analysis of space-time codes in spatially correlated fading channels* by T. A. Lamahewa, M. K. Simon, T. D. Abhayapala, and R. A. Kennedy, and *CDMA wireless system with blind multiuser detector* by W. Y. Leong and J. Homer report on research into techniques for better bandwidth utilization and interference mitigation in wireless systems. Such techniques will be necessary for the future wireless networks to accommodate ever growing number of users with increased bandwidth demands caused by the multimedia applications.

The final paper of the issue *A highly accurate DFT-based parameter estimator for complex exponentials* by J. Tsui and S. Reisenfeld describes a low complexity algorithm for the phase and amplitude estimation suitable for real time digital signal processing applications which are necessary for an accurate reconstruction of data from the received signal.

The guest editor would like to thank here all the authors for their contributions and the reviewers for their hard work in preparing their submissions, reviewing, and revising the papers on time.

Tadeusz Antoni Wysocki
Guest Editor

Paper

Gaze-J2K: gaze-influenced image coding using eye trackers and JPEG 2000

Anthony Nguyen, Vinod Chandran, and Sridha Sridharan

Abstract— The use of visual content in applications of the digital computer has increased dramatically with the advent of the Internet and world wide web. Image coding standards such as JPEG 2000 have been developed to provide scalable and progressive compression of imagery. Advances in image and video analysis are also making human-computer interaction multi-modal rather than through the use of a keyboard or mouse. An eye tracker is an example input device that can be used by an application that displays visual content to adapt to the viewer. Many features are required of the format to facilitate this adaptation, and some are already part of image coding standards such as JPEG 2000. This paper presents a system incorporating the use of eye tracking and JPEG 2000, called Gaze-J2K, to allow a customised encoding of an image by using a user's gaze pattern. The gaze pattern is used to automatically determine and assign importance to fixated regions in an image, and subsequently constrain the encoding of the image to these regions.

Keywords— eye tracking, image compression, importance map, JPEG 2000, region of interest.

1. Introduction

The use of visual content in applications of the digital computer, such as the Internet and world wide web, has increased dramatically in recent years. Image compression standards such as JPEG 2000 [1, 2] have been developed to provide scalable and progressive compression, and thus images can be displayed with varying resolution and quality depending on the bandwidth, memory and time available. Applications such as electronic commerce have become a reality, allowing merchandise in e-commerce to be displayed as images.

Advances in image and video analysis are also making human-computer interaction multi-modal, rather than through the use of a keyboard or mouse. New sensors and input devices such as the eye tracker have emerged. An eye tracker can locate on the monitor screen where a user is looking. Recent advancements in eye tracking technology, specifically the availability of cheaper, faster, accurate and user-friendly trackers, have inspired new research into eye movements and gaze patterns. Eye trackers are no longer intrusive or require cumbersome headgear to be worn.

Eye tracking can be used by an application that requires the display and adaptation of visual content to the viewer, provided the format in which the image is represented (coded) and reconstructed (decoded and displayed), and the environment (operating system extensions) in which the format is utilised can support such adaptation. Many features are required of the format to facilitate this and some are already a part of image coding standards such as JPEG 2000. Images can be encoded and decoded in JPEG 2000 with scalable resolution and quality in a progressively increasing manner, and regions of interest (ROI) can be selected in images and used to encode/decode the image in a non-uniform manner. This paper presents a system, called Gaze-J2K, which uses eye trackers and JPEG 2000 to allow an image author (i.e., user at the encoder) to use their gaze to automatically determine and assign importance to fixated regions in an image, and subsequently constrain the encoding of an image to these regions. This allows the user to receive the image as desired by the image author. This is very useful for the Internet and world wide web for applications such as merchandising, where faster interpretation of image contents would imply the faster rejection of unwanted images and hence improve user productivity.

2. Gaze-J2K system overview

The Gaze-J2K system incorporates a multi-modal interaction device provided by an eye tracker to allow an image author to influence and direct the encoding of an image to particular objects or ROIs in an image using JPEG 2000. The system comprises of three stages of operation as shown in Fig. 1, namely, gaze point collection, gaze point analysis and ROI prioritised JPEG 2000 image coding. Here the gaze point collection stage records information on the location and sequence of regions in an image followed by the image author. The structure of the spatial and temporal characteristics of the gaze pattern can then be used as parameters and analysed to generate ROIs and its measure of importance. These ROIs and importance scores define a ROI "importance" map, which can be input to a JPEG 2000 ROI encoder to prioritise the image code-stream according to the importance map specification. A client at the decoding end can receive the image progressively with the default ROIs, which were considered important by the image author, reconstructing faster than other regions in the image. Each stage of operation is described in further detail in the following sections.

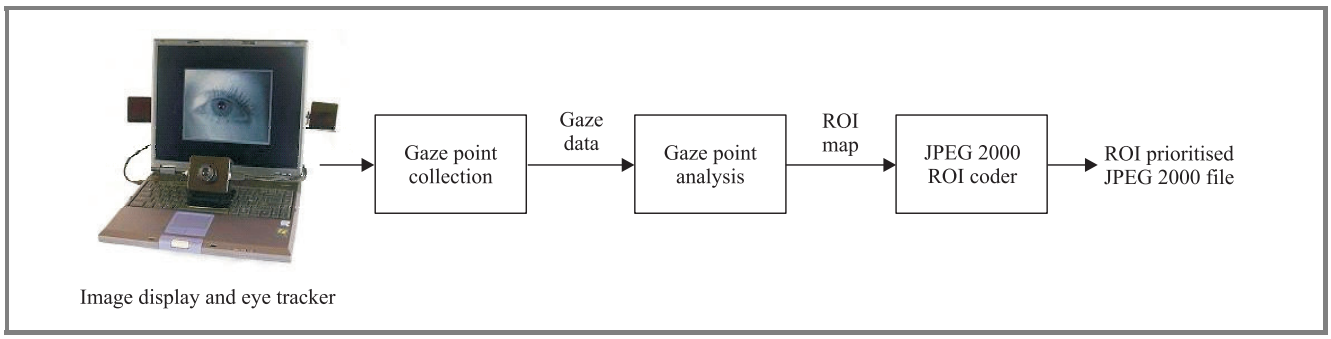


Fig. 1. Gaze-J2K system block diagram.

3. Gaze point collection

The goal of gaze or eye tracking is to determine the gaze point on the field of view where a user is looking. The device used to record eye movements was an EyeTech video-based corneal reflection eye tracker [3]. Infrared lights were mounted on both sides of a computer monitor to illuminate the eye and provide reference points for the eye tracker. The method of operation relies on focusing and tracking the infrared reflections from a user's eye using an image sensing camera mounted in front of the monitor screen. By analysing the position of the infrared light reflections and the center of the pupil contained in the image captured, the gaze point can be determined. The gaze-tracker can operate at 15 to 30 frames per second (fps) and records the position and time of gaze. The system was setup so that gaze data collection can be conducted on an image and screen resolution of 1024×768 pixels.

Number of recorded samples

1 second of gaze data

```
150
  0   551   473  -10375     0
  1   537   464      70 10445
  2   514   297     100    30
  3   514   301     150    50
  4   509   301     220    70
  5   504   280     290    70
  6   505   280     350    60
  7   505   286     421    71
  8   510   288     491    70
  9   511   288     551    60
 10   511   366     621    70
 11   502   384     691    70
 12   503   384     751    60
 13   503   379     821    70
 14   468   383     891    70
 15   469   383     951    60
 16   480   383    1021    70
 17   480   383    1091    70
 18   473   372    1152    61
 19   492   342    1222    70
 20   579   342    1292    70
```

Fig. 2. Example eye tracker gaze data output (extract).

An example extract of a recorded gaze data output by the eye tracker at 15 fps is shown in Fig. 2. The first line of the recorded gaze data shows how many samples were recorded. Each line thereafter contains information for one gaze point, which details the sample number, x-position (pixels), y-position (pixels), time from start (ms), and time from last sample (ms). The position and time information provided by the gaze data provides a couple of parameters that can be used to analyse the gaze pattern and determine, if any, ROIs fixated by the viewer.

A collection of gaze data were obtained from 13 subjects, of which 11 were naive to the purpose of the study. Six colour images (boat, cow, horse, paddock, rockclimb, and yacht), each with at least one primary object of interest clustered in a scenic background as shown in Fig. 3 (in this edition black-white), were displayed on the computer monitor, and each subject was told to locate and examine the objects in the image. For each image, the task was repeated three times for a duration of 15 seconds each. The eye tracker sample rate was set to 20 fps.

A few problems can occur at this stage of the Gaze-J2K process due to the eye tracker failing to track the infrared reflections or the pupil of the eye. As a result, the number of gaze points recorded by the eye tracker can be considerably less than normal. Drifts in the location of the gaze points cause by the tracking of the infrared reflections can also correspondingly produce an offset relative to the actual location fixated. If this offset is large enough, then subsequent stages of Gaze-J2K will generate a ROI map that will not correspond to the ROI. Minor drifts, however, will not adversely affect the results.

A culling process was performed to discard gaze data sets that were found to be unsuitable for further processing. A total of 229 out of the 234 gaze patterns were retained for the testing of subsequent stages of Gaze-J2K. These discarded gaze data sets were mainly due to the eye tracker failing to locate the viewer's location of fixation for the vast majority of the viewing duration.

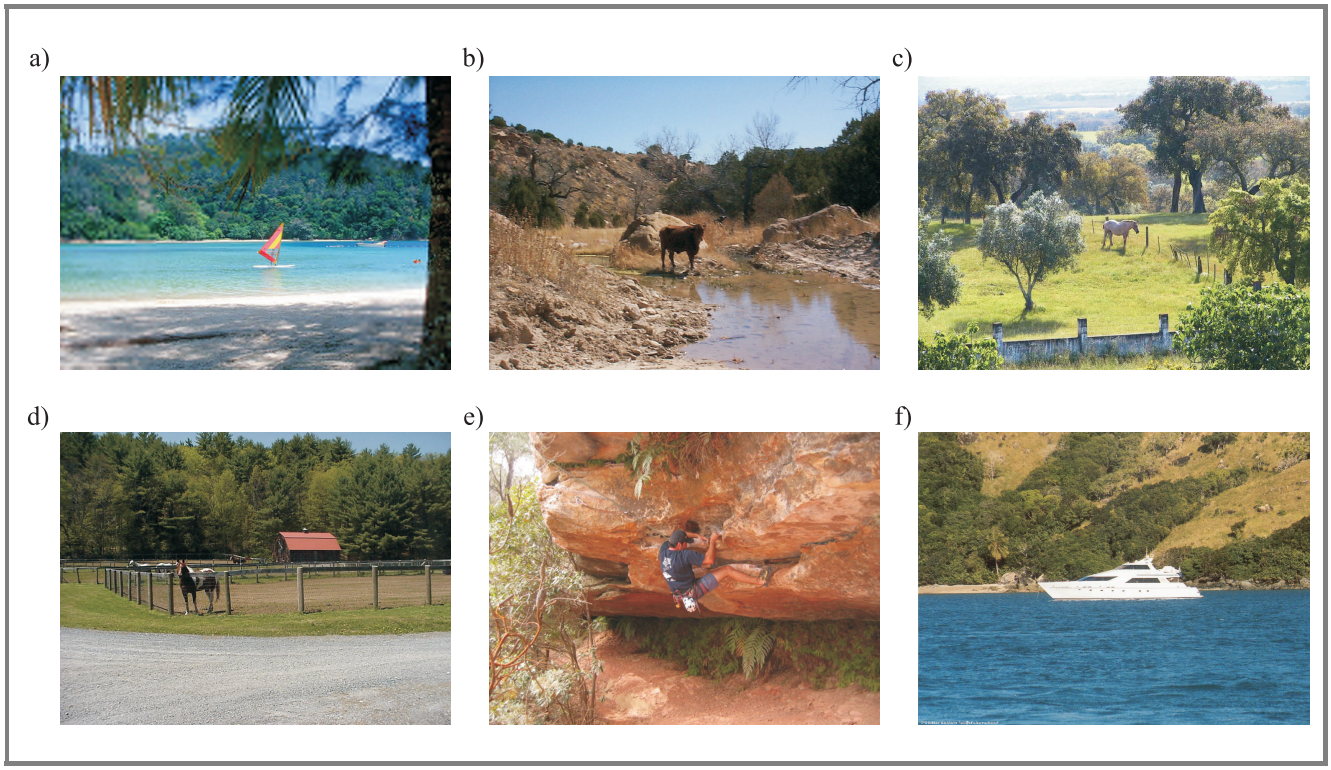


Fig. 3. Gaze-J2K colour test images (1024×768, 24 bpp): (a) "beach"; (b) "cow"; (c) "horse"; (d) "paddock"; (e) "rockclimb"; (f) "yacht".

4. Gaze point analysis

The purpose of gaze point analysis is to analyse a viewer's gaze pattern to determine ROIs fixated by the viewer. This procedure reduces the spatial characteristics of the gaze pattern to a limited subset of clusters that would represent ROI candidates. The choice of clustering technique is influenced by a number of factors such as whether the probability densities of the data are known or can be modelled, and the size of the data set. Since the number of gaze location points are limited and its spatial distribution is unknown, an unsupervised clustering technique, such as K-means, was used. In addition to the clustering procedure, a means to determine the importance of the ROI candidates was also investigated. The following subsections detail the development of the ROI clustering and ROI mapping stages.

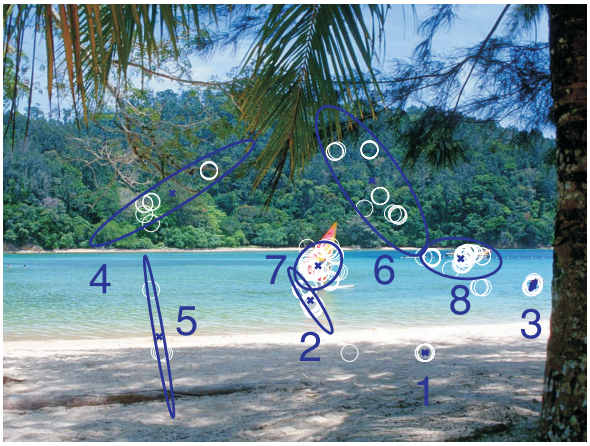
4.1. ROI clustering

The ROI clustering involves the partitioning of gaze points into mutually exclusive clusters such that the loci of the points belonging to the clusters represent ROI candidates for the particular gaze pattern. Here, a K-means clustering method is used to assign data to one of K clusters using the distance from the means of these clusters. A data vector is assigned to the nearest cluster mean. After all data vectors are classified, the means are updated using the sample means of the data vectors assigned to that cluster. The process is iterated until convergence (i.e., the means do not change significantly when compared against a precision threshold). The result is a set of clusters that are as compact and well-separated as possible. The K initial values for the cluster means were chosen randomly from the data set. These initial values can cause K-means to converge to a local minima, where the total sum of distances are a minimum, from which a better solution may exist. To avoid this, K-means was repeated a number of times and if different local minimums exists then the case with the lowest total sum of distances, over all repetitions, was returned.

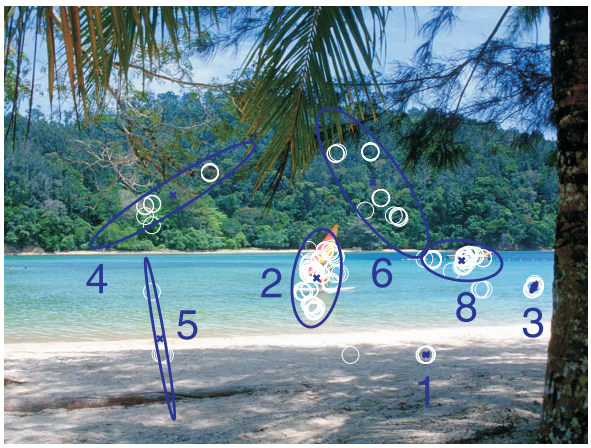
The value K can be arbitrarily chosen based on examination of the gaze tracking data, or simply by increasing the number of clusters to see if K-means can find a better grouping of the data. One method to automatically determine K is to determine how well-separated the resulting clusters are and choose a K which gives maximum separation. A silhouette score can be used to measure how close each point in one cluster is to points in neighbouring clusters. This measure ranges from $+1$, indicating that the points are very distant from neighbouring clusters, through to 0, indicating points that are not distinctly in one cluster or another, to -1, indicating points that are probably assigned to the wrong cluster. The average of the silhouette scores for each K can be used as a quantitative measure to compare different K's. In this paper, K-means was repeatedly performed by increasing K by 1 at each stage until the silhouette score for the grouping of data for $K+1$ is less than that for K. In such a case, K would give a maximum silhouette score

a)

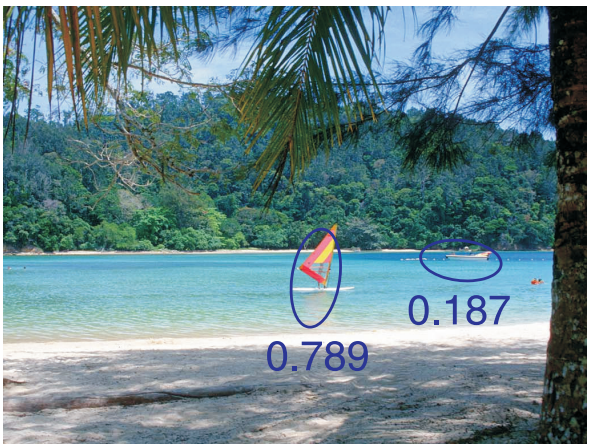
b)



c)



d)



e)

ROI cluster	1	2	3	4	5	6	7	8
Importance score *	0.001	**0.789**	0.002	0.004	0.000	0.017	NA	**0.187**
* Values in bold are above the ROI threshold of 0.15 and are retained for ROI prioritisation.								

Fig. 4. An illustrated example of the ROI clustering and mapping process: (a) gaze locations (circles) recorded by an eye tracker; (b) output of K-means clustering process showing cluster loci of ROI candidates (ellipses); (c) set of ROI cluster candidates after merging of close clusters; (d) final ROI importance map output after culling of "unimportant" clusters; (e) importance scores using the *visit weighted (cluster count)*^{2} metric for the clusters shown in Fig. 4c.

and the data vectors and mean of the clusters that correspond to K would represent the "best" grouping of the data.

In some cases, several clusters may be close together and a procedure is required to merge the two clusters. The rule used to merge was if any two cluster means fall within a distance threshold of 10% of the average of the image dimensions, then the two clusters would merge into one. The merging process would often merge multiple clusters belonging to the same object into a single cluster. The number of clusters, K, and the cluster mean are updated as the clusters are merged.

The cluster means and covariances of the data vectors that were assigned to the clusters were used to generate ellipses to represent the loci of ROI candidates. The major and minor radial components of the ellipses were chosen to be 2.58 standard deviations in each direction. In such a case, if the cluster's spatial distribution was Gaussian, then this will represent approximately 99% of data points belonging to the cluster. The total ROI size (area bounded by all the ellipses) was also restricted to less than 25% of the image space. This is to ensure that during the encoding process, the reconstructed quality of ROIs more than compensates for the overhead in encoding the ROI [4]. If the ROI area did not satisfy this condition, then the process was repeated using $K = K + 1$.

An illustrated example of the ROI clustering process using the "beach" image is shown in Fig. 4. The "beach" im-

age contains a number of objects of interest that a viewer may gaze upon, namely the windsurfer and perhaps the boat and people swimming (towards the right hand side of the image). For a particular viewer, the location of gaze points recorded by the eye tracker are shown in Fig. 4a. The plot does not contain any information about the sequence these points were viewed in. Figure 4b shows the grouping of data output by the clustering process described above. In the case shown, the number of clusters that resulted in a maximum silhouette score was $K = 8$. Finally, as shown in Fig. 4c, the set of clusters was refined by merging clusters whose geometric means were close together. In the example shown, cluster 2 was merged with cluster 7 and the new cluster mean and loci were recomputed.

The quality of the ROI clustering results is very dependent on the gaze data being clustered. If the ROI in an image is large, such as those in the "rockclimb" and "yacht" image, then multiple clusters may result for the single object. There were also cases where viewers only fixated on a particular region of a ROI, such as the head of the cow, which meant that the clustering procedure will not produce a ROI loci which would encompass the whole object. Other problems that may exist is that some gaze points not belonging to the ROI may be included in the ROI cluster simply because the gaze point was closer to the ROI cluster than any other clusters. These problems can be overcome by improving the clustering algorithm to reduce the sensitivity of "outlier" gaze points and/or by having viewers get more experience with the eye tracker hardware and be more aware of the purpose of the task required for the application at hand. Since most viewers were naive to the purpose of the gaze tracking experiment, a diversity in range of gaze patterns resulted.

4.2. ROI mapping

Given that the ROI clustering procedure outputs K candidate ROIs, a ROI mapping procedure is required to assign an importance measure or score to each ROI. This importance score can be interpreted as the degree of importance of the ROI relative to other regions in an image. Regions with a high importance score represents regions of high importance, which should be retained and prioritised by the encoder with higher priority than regions with a low importance score, which are to be removed and prioritised along with the image background.

It is conjectured that the fixation-saccade sequence provided by the gaze patterns would reveal underlying visual attentional processes that can be used to develop an importance metric. Several factors have been previously considered such as cluster count, distance, variance, area, and revisit count, and were combined using an entropy weighting procedure to weight each factor accordingly [5]. The ROI mapping procedure was found to be sound for the gaze data and particular test image. Here, such a complex metric may not be appropriate to model an importance metric that would suit all viewers and gaze patterns.

In this paper, a subset of factors which are intuitive from the gaze pattern sequences are studied. This includes the count or duration of gaze points belonging to a cluster and it's sequential behaviour in terms of the number of visits and revisits to a given cluster. These factors provide several possible derivations for an importance metric. The importance measures investigated in this paper are *cluster count*, $(\textit{cluster count})^2$ and *visit weighted* $(\textit{cluster count})^2$.

The *cluster count* measures the number of gaze points that belong to a given cluster. This factor is analogous to the duration of gaze within the cluster, since uniform gaze sampling was recorded. This factor represents the total time spent viewing/gazing at that region. The cluster's count was mapped to a range 0 to 1 by dividing the measures by its sum. The mapped range indicates a cluster's relative importance for the given metric.

To determine whether or not a cluster is classified as a ROI or not, a threshold of 0.15 was applied to the measures. A cluster importance measure greater than 0.15 would be retained and considered as an ROI, else the clusters would be considered as part of the background for ROI coding purposes. The threshold was chosen such that the number of clusters classified as a ROI, in general, would be slightly larger than the number of "actual" ROIs. This would minimise the number of ROIs that would be misclassified, while taking into account the fact that each ROI may contain a number of clusters.

The performance of the metric was evaluated in terms of ROI misses and ROI false alarms. ROI misses are those cases where the ROI mapping algorithm did not pick up a primary object of interest in an image as an ROI, while a ROI false alarm is the case where the algorithm considered a cluster as a ROI when it contains no object of interest. Because of the varied range in objects fixated by a viewer and the number of objects that may exist in an image, an "intuitive" rule-based ROI definition was formulated to define the ROI. The following rule-based definitions were used:

- "Beach" image – ROI must contain the windsurfer. The boat and people swimming on the right of the image were not considered as ROI false alarms.
- "Cow" image – ROI must contain the cow.
- "Horse" image – ROI must contain the horse.
- "Paddock" image – ROI must contain the horse in the foreground. The horses in the background and the barn are not ROI false alarms.
- "Rockclimb" image – ROI must contain the upper body of the rock climber. The rock climber's lower body were not considered to be a ROI false alarm.
- "Yacht" image – ROI must contain at least the centre of the yacht. Other parts of the yacht were not ROI false alarms.

With the above ROI definition, the *cluster count* metric contained 20 ROI misses and 48 ROI false alarms. The square

of the number of cluster gaze points, $(cluster\ count)^2$, was found to be a more useful metric as it emphasises regions with a high cluster count and penalises those with a small cluster count. This resulted in a much improved ROI performance with 13 ROI misses and 41 ROI false alarms.

Furthermore, it was hypothesised that by making use of the number of visits (or revisits) to a given cluster during the course of viewing would provide additional information to determine the cluster's importance. The more visits to a given cluster, the more important the cluster should be. The *visit weighted (cluster count)*^{2} metric is given by the square of the number of cluster gaze points multiplied by n, where n is the number of visits to the cluster under consideration. To stop those clusters with a high number of visits from having a dominant effect on the cluster importance, the visit weight was capped at 3. This value was chosen since clusters with a number of visits greater than 3 were statistically unreliable with on average less than 1 cluster per gaze pattern with a number of visit greater than 3.

Table 1 shows the performance in terms of ROI misses and ROI false alarms for the three ROI mapping methods. It can be seen that *visit weighted* $(cluster\ count)^2$ improves the ROI performance even further by reducing the ROI misses to 7, while only marginally increasing the number of ROI false alarms.

Table 1
The ROI misses and ROI false alarm results for three ROI mapping metrics *

Importance metric	Number of ROI misses	Number of ROI false alarms
Cluster count	20 (8.7%)	48 (21.0%)
(Cluster count)^2	13 (5.7%)	41 (17.9%)
Visit weighted $(cluster\ count)^2$	7 (3.1%)	45 (19.7%)

* Values in parentheses are percentages of the total number of gaze data.

It should be noted that the majority of ROI misses and ROI false alarms are contributed by only a few viewers. Table 2 provides an indication of the distribution of ROI misses and ROI false alarms across the viewers for the *visit weighted* $(cluster\ count)^2$ metric. Notice that only two viewers contributed to the ROI misses, while a varying amount of ROI false alarms were contributed by different viewers. The large number of ROI false alarms indicates that viewers have their own viewing preferences and fixated on other regions in addition to the defined ROIs. As suggested earlier, the ROI performances can be improved if the viewers had more experience with the eye tracker and were more informed of the purpose of the task that was required.

The importance scores using the *visit weighted* $(cluster\ count)^2$ metric for the illustrated example shown in Fig. 4c is tabulated in Fig. 4d. The cluster importance scores that are in bold font represents those clusters retained as an ROI (i.e., importance score > 0.15). Note that only the windsurfer and the boat are retained as ROIs and represents the objects of interest found important for the particular viewer. The degree of importance is represented by the value of the importance score.

The duration and order of the cluster visits were also considered but the results did not provide an improved ROI performance over the *visit weighted* $(cluster\ count)^2$ case. Viewer's gaze patterns were too varied and these measures did not apply globally across all gaze data sets. If the underlying visual attentional processes of each viewer can be known, improved performances can be gained.

5. JPEG 2000 ROI image coding

The coding/decoding of images may be influenced to enhance the image quality in ROIs. JPEG 2000 provides several ROI coding mechanisms which can prioritise predefined ROIs, such as the max-shift [1, 2] and implicit [2] ROI coding methods. The problem with these methods are that implementations, such as that in [6], treat all ROIs with the same degree of importance and thus all pre-defined ROIs will be emphasised and prioritised with the same level of priority regardless of their degree of importance. To overcome this, an importance prioritised JPEG 2000 (IMP-J2K) image coder [7, 8] was developed to extend the concept of the Implicit method to incorporate an importance map to quantitatively model multiple ROIs and variable ROI importance scores. With IMP-J2K, the ROI was emphasised by weighting the mean square error (MSE) distortion measure of a block of coefficients by the square of its importance score. The reconstruction of the ROIs are bounded by the extent of these blocks. This is advantageous for the ROIs generated from the clustering process, since the ROIs may not fully encompass the objects in the image.

The ROI cluster loci and importance measures as generated by the ROI mapping stage can be input to IMP-J2K for ROI encoding, with an additional background importance parameter of, say, 0.01. Figure 5 shows an example of reconstructed images as the ROI encoded image is progressively (or incrementally) transmitted and received by the recipient for the illustrated example in Fig. 4. Note that only cluster 2 and 8 (in Fig. 4) were prioritised and emphasised during the encoding process. The ROIs, especially the windsurfer, can be observed to be reconstructed with better quality and at a higher resolution than the rest of the image, especially during the earlier stages of transmission when only a part of the code-stream has been received. However, when the entire code-stream has been received, the lossless (or near lossless) representation of the image is possible. The gaze-influenced selective coding of parts of an image provides a user of the image to receive the image as desired by the image author.

Table 2

The ROI misses and ROI false alarms contributed by viewers for the *visit weighted* (*cluster count*)^2 ROI mapping metric

Viewer	1	2	3	4	5	6	7	8	9	10	11	12	13	Total
Number of ROI misses	0	0	0	0	0	0	0	0	0	0	2	0	5	7
Number of ROI false alarms	0	1	1	8	6	1	0	3	4	0	4	7	10	45

Fig. 5. Progressive decoding of a ROI prioritised code-stream at: (a) 0.0625; (b) 0.125; (c) 0.25; (d) 0.5; (e) 1.0; (f) 2.0 bits per pixel (bpp) for the beach image example in Fig. 4. The ROIs improve most rapidly at reduced bit-rates, while the visually lossless (or near-lossless) reconstruction of the image as a whole is possible at higher bit-rates.

6. Conclusions

This paper has presented a system, called Gaze-J2K, which uses a combination of eye tracking and JPEG 2000 image coding, to allow an image author to customise the encoding of an image for users of an application. The system collects spatial and temporal gaze information from a viewer, uses the gaze pattern to automatically locate and assign importance to a representative subset of ROIs, and subsequently encode these regions with higher priority. Experimental results show that the accuracy of determining ROIs can be as high as 97% and can be further improved for experienced viewers. The system can be used in various applications such as the Internet and world wide web, which require the display of visual content to adapt to the end user.

References

[1] "Information technology – JPEG 2000 image coding system – Part 1: Core coding system," ISO/IEC 15444-1, Aug. 2002.

[2] D. S. Taubman and M. W. Marcellin, *JPEG 2000: Image Compression Fundamentals, Standards, and Practice*. Boston: Kluwer, 2002.

[3] EyeTech Digital Systems, "Quick glance eye-gaze tracking system", 2005, http://www.eyetechds.com/

[4] A. P. Bradley and F. W. M. Stentiford, "JPEG 2000 and region of interest coding," in *Proc. Digit. Im. Comput. Techn. Appl.*, Melbourne, Australia, 2002, pp. 303–308.

[5] A. Nguyen, V. Chandran, and S. Sridharan, "Visual attention based ROI maps from gaze tracking data," in *Proc. Int. Conf. Im. Proces.*, Singapore, 2004, pp. 3495–3498.

[6] D. Taubman, "Kakadu software: a comprehensive framework for JPEG 2000", 2005, http://www.kakadusoftware.com/

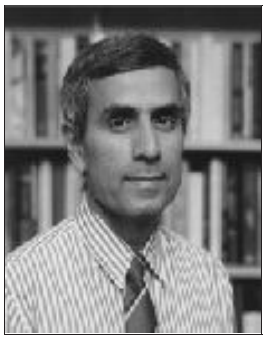
[7] A. Nguyen, V. Chandran, and S. Sridharan, "Importance prioritisation in JPEG 2000 for improved interpretability," *Sig. Proces. Im. Commun.*, vol. 19, no. 10, pp. 1005–1028, 2004.

[8] A. Nguyen, "Importance prioritised image coding in JPEG 2000", Ph.D. thesis, School of Engineering Systems, Queensland University of Technology, Brisbane, Australia, Jan. 2005.

Anthony Nguyen received the B.E. (aerospace avionics) degree with first class honours in 1999, and a Ph.D. degree in the area of image processing and image compression in 2005 from Queensland University of Technology (QUT), Brisbane, Australia. He is currently a Research Fellow within the Image and Video Research Laboratory, School of Engineering Systems at QUT. He is also a tutor and a telecoms lab development coordinator for the digital communications and wireless communications units. His research interests include image processing, image compression, and pattern recognition. He is a Member of the Institute of Electrical and Electronic Engineers – IEEE (USA).

e-mail: a.nguyen@ieee.org
Image and Video Research Laboratory
School of Engineering Systems
Queensland University of Technology
GPO Box 2434, Brisbane QLD 4001, Australia

Vinod Chandran received the B.T. degree in electrical engineering from the Indian Institute of Technology, Madras, India, in 1982, the M.Sc. degree in electrical engineering from Texas Tech University, Lubbock, in 1985, and the Ph.D. degree in electrical and computer engineering and the M.Sc. degree in computer science from Washington State University, Pullman, USA, in 1990 and 1991, respectively. He is currently an Associate Professor at the Queensland University of Technology (QUT), Brisbane, Australia, in the School of Engineering Systems. His research interests include pattern recognition, higher order spectral analysis, speech processing, and image processing. He is a Senior Member of the Institute of Electrical and Electronic Engineers – IEEE (USA) and the Chairman of the IEEE Computer Society in Queensland.
e-mail: v.chandran.qut.edu.au
Image and Video Research Laboratory
School of Engineering Systems
Queensland University of Technology
GPO Box 2434, Brisbane QLD 4001, Australia



Sridha Sridharan has a B.Sc. (electrical engineering) degree and obtained a M.Sc. (communication engineering) degree from the University of Manchester Institute of Science and Technology (UMIST), UK, and a Ph.D. degree in the area of signal processing from University of New South Wales, Australia. He is currently with the Queensland University of Technology (QUT), where he is a Professor in the School of Engineering Systems. He is also the Program Leader of the Research Program in Speech, Audio and Video Technology at QUT. In 1997, he was the recipient of the award of Outstanding Academic of QUT in the area of research and scholarship. He is a Fellow of the Institution of Engineers, Australia, a Senior Member of the Institute of Electrical and Electronic Engineers – IEEE (USA) and the Chairman of the IEEE Queensland Chapter in Signal Processing and Communication.
e-mail: s.sridharan@qut.edu.au
Image and Video Research Laboratory
School of Engineering Systems
Queensland University of Technology
GPO Box 2434, Brisbane QLD 4001, Australia

Paper

Benchmarking image codecs by assessment of coded test images: the development of test images and new objective quality metrics

Amal Punchihewa, Donald G. Bailey, and Robert M. Hodgson

Abstract— Objective quality measures are required for benchmarking codec performance. Our aim was to develop a simple, accurate method capable of rapidly measuring the degree of blockiness, edge-blur and ringing due to image compression. Two test images were designed to emphasise these artefacts. The efficacy of the new metrics is demonstrated using a JPEG codec at a range of compression levels.

Keywords— image quality, artefacts, subjective, objective, coding, metric, blockiness, blur, ringing.

1. Introduction

Lossy image and video compression codecs introduce many types of distortions known as artefacts. *The Digital Fact Book* defines artefacts as "particular visible effects, which are a direct result of some technical limitation" [1]. Artefacts are generally not evaluated by traditional methods of signal evaluation. For instance, the visual perception of contouring in a picture cannot be related to signal-to-noise ratio [1].

In multimedia communications, image and video are the dominant components. With limited communication bandwidth and storage capacity in terminal devices, it is necessary to reduce data rates. High levels of compression result in undesirable spurious features and patterns in the reconstructed image; these are the artefacts defined above. Image compression schemes such as JPEG use the techniques of discrete cosine transform (DCT), block processing and quantisation. This may result in blockiness, edge-blur, contouring and ringing artefacts in coded images. The following table summarises these artefacts.

When the original signal is not fully known, quantifying these artefacts is difficult. In particular, it is difficult to isolate the individual components listed in Table 1.

Image codec development, parameter tuning and benchmarking all require availability of more accurate and swift measurements. Subjective assessment can provide an accurate indication of perceptual quality but such methods are very time consuming [3]. Traditional full referenced metrics such as mean square error (MSE) and peak signal to noise ratio (PSNR) do not always correlate well with perceptual quality, and are unable to distinguish between different types of artefacts [3].

Researchers have developed objective quality metrics for different artefacts based on non-referenced or reduced reference techniques [3–5]. They are good for in-service measurements and estimates, as they are not as accurate as full-referenced methods. Bailey *et al*. proposed a non-referenced, objective, quality metrics for blockiness based on edge activity of reconstructed images [4].

Table 1
Summary of common artefacts found in digital image and video systems [2]

Artefact	Description
Blockiness	Distortion of the image characterized by the appearance of an underlying block structure.
Edge-blur	Distortion, characterized by reduced sharpness of edges.
Ringing	Appears as echoes of the hard edges in the picture or a rippling adjacent to step edges.
Contouring	Visibility of bands of intensity over large regions.

If the original image is unknown it is often difficult to determine the presence and extent of artefacts. Therefore the approach in this paper is to use the full referenced method using synthetic images having known spatial distributions of pixel values designed to emphasise the artefacts to be assessed. This study is concentrated primarily on three of the most common coding artefacts, namely blockiness, edge-blur and ringing. A search of the literature did not reveal any full-referenced objective quality metric and accompanying test images for blockiness, ringing or edge-blur.

2. Methodology

The main aim of this full referenced quality assessment approach was to design and synthesise a few test patterns in which the spatial distribution of pixel values will emphasise artefacts due to codec operation. Many image compressors have a control parameter, the quality factor that

can be set by the user to adjust the compression ratio. In general the lower the quality factor the higher the compression ratio and the more visible artefacts become. At low compression ratios, the artefacts may not be obvious to the human eye.

2.1. Definition of quality metrics

2.1.1. Blockiness

Blockiness is the distortion of the image characterised by the visibility of the underlying block encoding structure [4]. Some codecs, such as JPEG, divide the image into a number of small blocks which are then processed independently. As there are no constraints applied between adjacent blocks, such processing can result in discontinuity in reconstructed pixel values at block boundaries. The visibility of the block encoding structure depends on the magnitude of the discontinuity in the reconstructed image and can be measured horizontally and vertically as pixel intensity difference at block boundaries.

The proposed blockiness objective quality metric is more suitable for codecs complying with the JPEG standard. The proposed objective quality metric assumes a block size of 8×8, the typical block size in JPEG codecs. JPEG 2000 standard has the provision to divide an image into rectangular blocks of the same size called tiles. Each tile is encoded independently. Tile size is a coding parameter that is explicitly specified [6]. This may result in a blocky appearance however is not considered in this research.

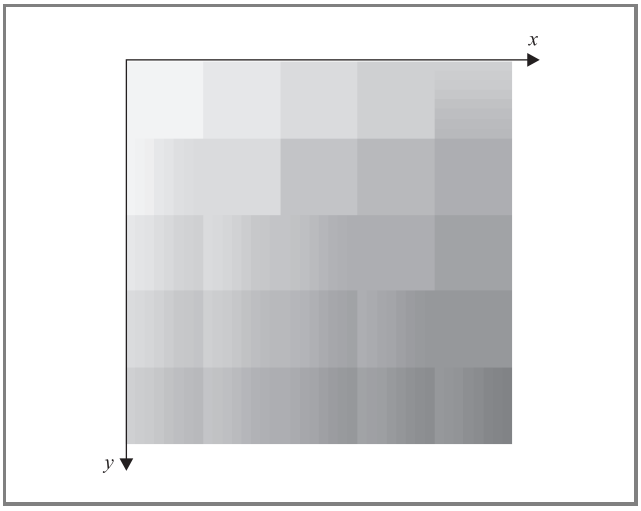


Fig. 1. Example of blockiness resulting from JPEG codec at high compression ratio in the spatial domain.

Blockiness can be expressed as the discontinuity in amplitude per block boundary pixel in the image. The higher the value of the blockiness, the higher the visibility of block structure.

Consider an $M \times N$ image I, reconstructed from a 8×8 block coded image having M rows and N columns. As shown on Fig. 1, both vertical and horizontal edges can be observed at regular pixel intervals of 8 because of the 8×8 block processing. Consider row y, along line y, the horizontal blockiness can be calculated as

$$\sum_x \left| I[x,y] - I[x+1,y] \right|,$$

where $x = 8, 16, 24, \ldots, (N-8)$. This computation is repeated for all rows from $y = 1$ to M. The total of the vertical blockiness VB can be written as

$$VB = \sum_{y=1}^{M} \sum_x \left| I[x,y] - I[x+1,y] \right|. \tag{1}$$

This results from $\frac{(N-8)}{8} M$ block boundary pixels. Similarly, the horizontal blockiness HB,

$$HB = \sum_{x=1}^{n} \sum_y \left| I[x,y] - I[x,y+1] \right|, \tag{2}$$

results from $\frac{(M-8)}{8} N$ block boundary pixels.

Both the HB and the VB can be combined and normalised by dividing the number of boundary pixels. Hence the blockiness per boundary pixel B can be expressed as

$$\begin{aligned} B &= \frac{HB+VB}{\frac{N-8}{8}M + \frac{M-8}{8}N} \\ &= \frac{4(HB+VB)}{NM-4(M+N)}. \end{aligned} \tag{3}$$

2.1.2. Edge-blur and ringing

Ringing always occurs at edges and blur generally occurs at edges. Since we are concerned with the blur occurring at an edge, this paper concentrates on the edge-blur rather than a global-blur.

Ringing is an undesirable visible effect around edges. Many codecs transform the pixel values into the frequency domain where the transformed coefficients are then quantised. Quantisation errors resulting from this approach give rise to ringing around sharp discontinuities in the image.

An ideal sharp edge contains components at all frequencies. Any change in the amplitude of any of these components will result in ripples in the image with amplitude corresponding to the error.

As a result of energy compaction in a codec, many of the high frequency components are very small, and get quantised to zero. This loss of high frequency components leads to blur in reconstructed image.

Ringing and edge-blur are defined in Fig. 2. We define the region between the first crossings on each side of the edge transition as the edge-blur region. Outside of this, from the start of the first overshoot on each side, the errors are classified as ringing.

To obtain a measure of edge-blur, consider the shaded area in Fig. 2. The greater the edge-blur, the larger will be the shaded area. By dividing the area by the step height,

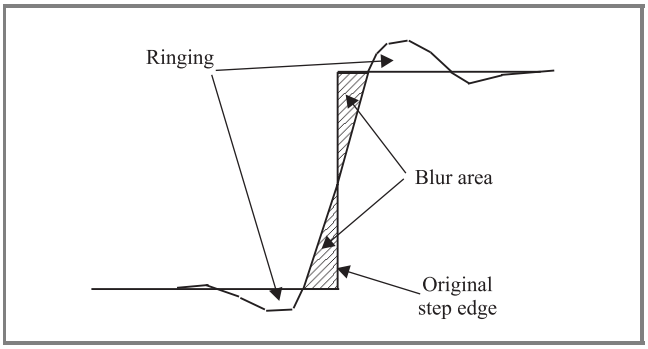


Fig. 2. Ringing and edge-blur at an edge of a one-dimensional signal.

a measure of average edge-blur width can be obtained. In a similar manner, the area between the ringing signal and ideal signal provides a measure of the severity of ringing. With sampled data, an ideal step edge would involve a transition between two pixels, as illustrated by the circles in Fig. 3.

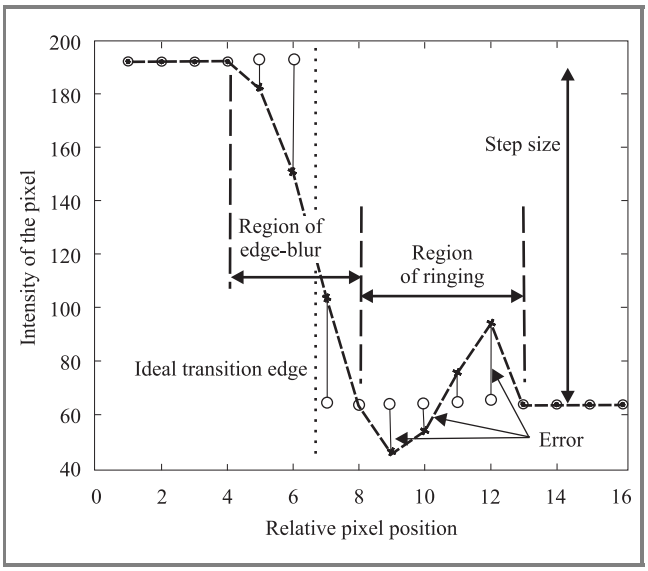


Fig. 3. Edge-blur and ringing for one-dimensional sampled data. Circles represent original pixel value and cross represent reconstructed pixel value.

The crosses in Fig. 3 are the pixel values near the edge of the reconstructed image from a codec. The transition from one intensity to another intensity involves many pixels. The pixel values of reconstructed image outside the region of edge-blur may oscillate around each intensity level of pixels of the original edge.
The edge-blur and ringing are therefore quantified as

$$\text{edge-blur} = \frac{\sum_{\text{blur\_region}} |\text{error}|}{\text{step size}}, \tag{4}$$

$$\text{ringing} = \frac{\sum_{\text{ringing\_region}} |\text{error}|}{\text{step size}}. \tag{5}$$

In 2D images, edges may appear at any orientation. Therefore we consider edge-blur and ringing perpendicular to the edge under consideration. By summing the Eqs. (4) and (5) over whole image and dividing by the number of edge pixels, we can obtain a measure of edge-blur and ringing per edge pixel.

2.2. Design of the test signals

Two simple synthetic test signals have been designed to emphasise visible edge-blur, ringing and blockiness artefacts. The pixel values and the shape of the pattern have been carefully chosen so that the algorithm could detect coding artefacts completely and adequately.

2.2.1. Blockiness

To generate and measure the blockiness artefact, it is necessary to have a test image without edges that results in edges at block boundaries after reconstruction. To produce such edges it is therefore necessary to have an intensity gradient within the test pattern. A simple horizontal or vertical gradient can not distinguish between edges introduced by block processing due to contouring resulting from too few quantisation levels. Therefore an intensity pattern was selected as shown in Fig. 4. The pixel values vary sinusoidally along a diagonal of the image. If pixel intensity varies linearly, the blockiness at certain compression ratios reduces. Nonlinear variation of pixel intensity of the test image (in form of sinusoidal function along a diagonal), stresses the codec at all compression ratios which is required to emphasise the blockiness artefact.

Fig. 4. Original diagonal test image, size: 66 614 bytes, bitmapped.

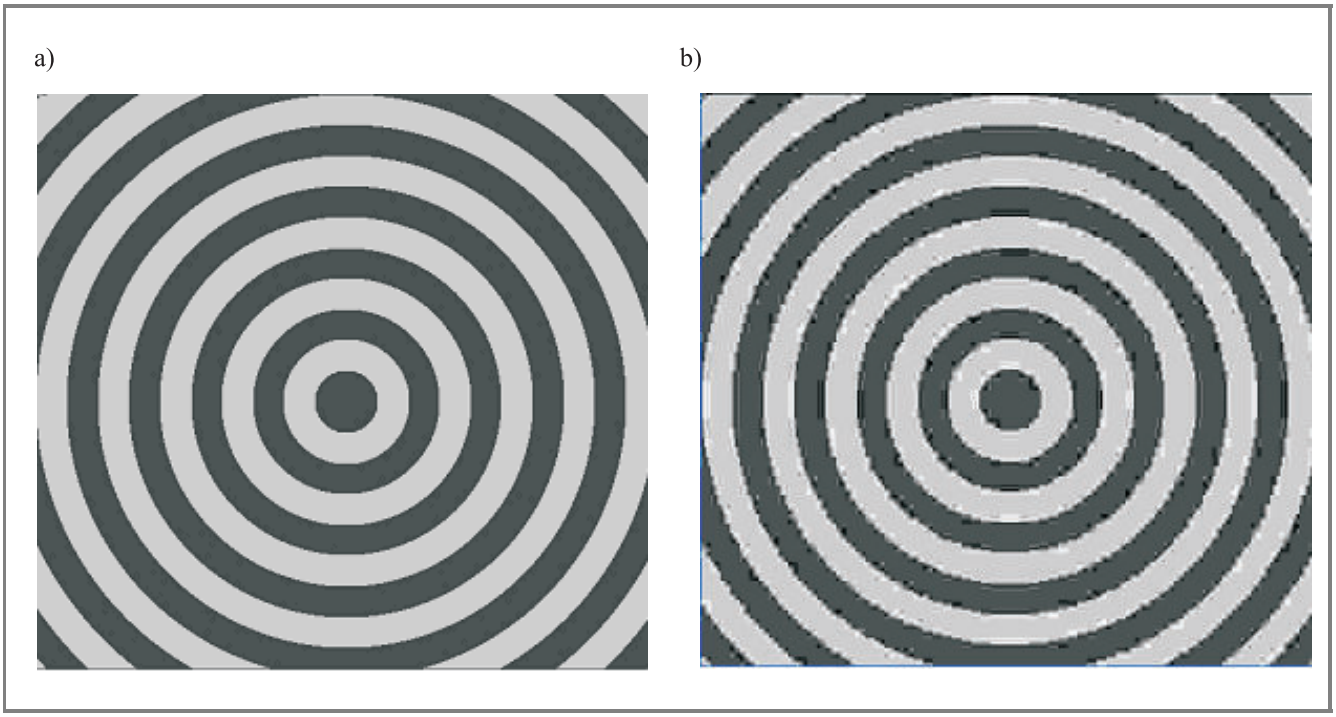


Fig. 5. (a) Original grey scale concentric test image and (b) JPEG reconstructed concentric circles test image with edge-blur and ringing.

Pixel values do not change uniformly within the test image with respect to their neighbours. The blockiness computation algorithm is applied to the error image; that is on the difference between original and reconstructed test image, to prevent the gradient within the original image being measured as blockiness.

2.2.2. Edge-blur and ringing

To test for edge-blur and ringing it is necessary to have step edges within the image. These should include edges of all orientations in order to detect any orientation sensitivity inherent in the codec. A circular pattern contains edges of every orientation. Pixel values of 64 and 192 have been chosen on either side of the boundary, so that after reconstruction there is adequate amplitude margin to allow for ringing in the reconstructed image. To allow for more edges and resulting error pixels, concentric circles have been incorporated (see Fig. 5). The spacing has been chosen as an odd number so that if block processing is used, the edges fall at different places within the blocks.

3. Results

The quality metrics were evaluated by applying them to the test images described in the previous section. The JPEG codec was tested at a range of compression ratios.

3.1. Blockiness

At low compression ratios the blockiness metric is small and increases rapidly with increasing compression ratio as shown in Fig. 6.

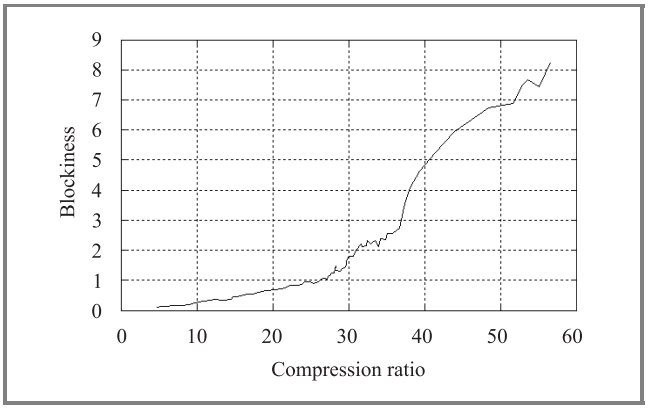


Fig. 6. Blockiness as a function of compression ratio using a JPEG codec on diagonal test image.

It was observed that errors not only occur at block boundaries but in some circumstances in the middle of blocks as well. This occurred at compression ratios of around 30 for this image, resulting in the minor non-monotonic variation seen in the results. This effect was particularly pronounced when a constant gradient image was used because of a threshold effect in quantising the JPEG coefficients.

At some compression levels, errors may actually reduce for higher compression depending on exactly where quantisation levels fall. The sinusoidal variation in the test image means that the different blocks have different gradients, averaging out, and significantly reducing, this effect.

3.2. Edge-blur and ringing

It can be observed that the general trend of ringing and edge-blur is upward with increasing compression ratio (Fig. 7). For the JPEG codec used for the simulations, ringing peaks around compression ratios of 10, 30 and 40.

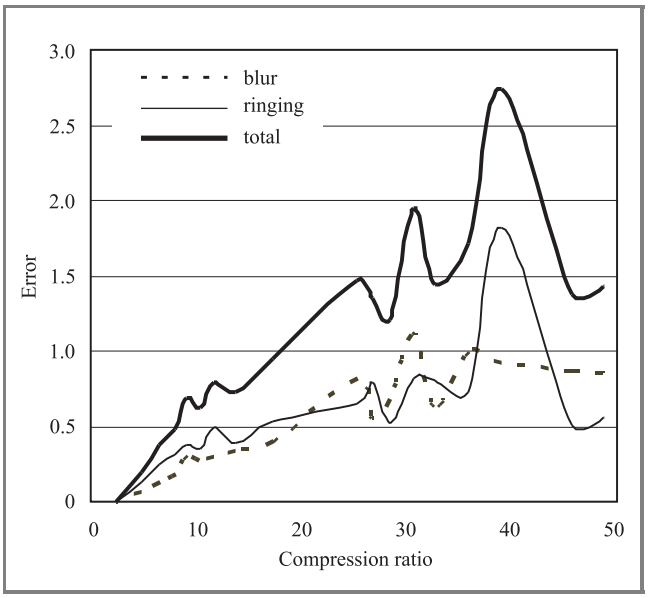


Fig. 7. Edge-blur, ringing metrics and total error as a function of JPEG compression ratio on the concentric circles test image.

These are due to quantisation errors which affect the dc component of the pixel values in reconstructed image around the edge. This has influenced the edge-blur around compression ratios 10 and 30. Edge-blur and ringing decrease above a compression ratio of 40 due to severe quantisation.

4. Conclusions

In this work three new objective quality measures for edge-blur, ringing and blockiness are proposed. The approach is based on known test patterns and measurements of the strength of each in the spatial domain. The quality metrics are good representations of artefacts and are swift in calculation. The proposed measures clearly distinguish between the three artefacts. The diagonal test signals were designed with knowledge of the specific mechanisms and weaknesses inherent in block-based transform coding. However, the concentric circles test image can be used to evaluate blur and ringing produced by any type of codec. The authors intend to perform further research to design test signals for measuring other types of artefacts (global-blur, colour artefacts, contouring) and extending to other types of codecs (JPEG 2000, MPEG, etc.).

References

[1] B. Pank, *The Digital Fact Book*. Berkshire: Quantel Limited, 2002.

[2] A. Punchihewa and D. G. Bailey, "Artefacts in image and video systems; classification and mitigation", in *Proc. Im. Vis. Comput*., Auckland, New Zealand, 2002, pp. 197–202.

[3] A. Punchihewa, D. G. Bailey, and R. M. Hodgson, "A survey of coded image and video quality assessment", in *Proc. Im. Vis. Comput*., Palmerston North, New Zealand, 2003, pp. 326–331.

[4] D. G. Bailey, M. Carli, M. Farias, and S. K. Mitra, "Quality assessment for block-based compressed images and videos with regard to blockiness artefacts", in *Tyrrhenian Int. Worksh. Dig. Commun.*, Capri, Italy, 2002, pp. 237–241.

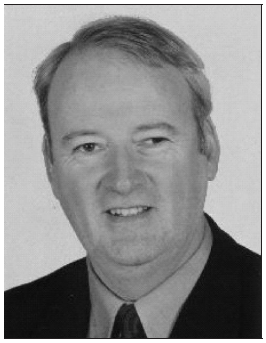
[5] M. Kusuma and H. Zepernick, "A reduced-reference perceptual quality metric for in-service image quality assessment", in *Proc. Internet, Telecommun. Sig. Proces. WITSP, Conf. & Worksh.*, Coolangatta, Australia, 2003, pp. 72–76.

[6] K. Varma and A. Bell, "JPEG 2000-choices and tradeoffs for encoders", *IEEE Sig. Proces. Mag.*, pp. 70–75, Nov. 2004.

Amal Punchihewa obtained his B.Sc. engineering degree specialising in electronic and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 1986. He received the Master of electronics engineering degree majoring in digital video signal processing from the Technical University of Eindhoven, The Netherlands, in 1991. He served as a computer hardware engineer, as the engineer research and planning at the national TV broadcaster in Sri Lanka, as a faculty member of the Faculty of Engineering at University of Moratuwa. As the head of engineering of the national TV broadcaster in Sri Lanka, he was instrumental in introducing many new technologies and infrastructure developments. He is a Fellow of IEE.

e-mail: g.a.punchihewa@massey.ac.nz
Institute of Information Sciences and Technology
Massey University
Private Bag 11222
Palmerston North, New Zealand

Donald G. Bailey has a B.E. (hons) and Ph.D. in electrical and electronic engineering from University of Canterbury. After spending 2 years applying image analysis techniques to the wool and paper industries within New Zealand, he spent 2 1/2 years as a visiting researcher at the Electrical and Computer Engineering Department at the University of California at Santa Barbara. In 1989, he returned to New Zealand as Director of the Image Analysis Unit at Massey University. In 1998 he moved to the Institute of Information Sciences and Technology, where he is currently senior lecturer and leader of the Image and Signal Processing Research Group.
e-mail: d.g.bailey@massey.ac.nz
Institute of Information Sciences and Technology
Massey University
Private Bag 11222
Palmerston North, New Zealand



Robert M. Hodgson holds a Bachelors degree and Ph.D. in electrical and electronic engineering and was trained in the UK avionics industry. After lecturing in electronic engineering at the University of Hull he joined the University of Canterbury in New Zealand in 1975. He was appointed Professor of information engineering at Massey University in 1988 and shortly after appointed the Head of the Department of Production Technology (Manufacturing and Information Technology). From 1998 to early 2004 he was the Head of Massey's Institute of Information Sciences and Technology. In 2004 he was appointed to be Director of the Massey School of Engineering and Technology.
e-mail: r.m.hodgson@massey.ac.nz
Institute of Information Sciences and Technology
Massey University
Private Bag 11222
Palmerston North, New Zealand

Paper

Application of convolutional interleavers in turbo codes with unequal error protection

Sina Vafi and Tadeusz A. Wysocki

Abstract— This paper deals with an application of convolutional interleavers in unequal error protection (UEP) turbo codes. The constructed convolutional interleavers act as block interleavers by inserting a number of stuff bits into the interleaver memories at the end of each data block. Based on the properties of this interleaver, three different models of UEP turbo codes are suggested. Simulation results confirm that utilizing UEP can provide better protection for important parts of each data block, while significantly decreasing the number of stuff bits.

Keywords— convolutional interleavers, unequal error protection, turbo codes.

1. Introduction

Unequal error protection (UEP) is introduced as an efficient technique for forward error correcting (FEC) codes to suitably protect encoded data based on their importance against channel errors. This is specifically utilized in the transmission of the compressed information such as voice, video and multimedia services which are very sensitive to bit and burst errors.

Among the known channel codes, turbo codes are introduced as effective FEC codes having good performance in error reduction. The turbo code is basically constructed by two recursive systematic convolutional (RSC) codes which are linked by an interleaver [1]. When the UEP property is implemented for the turbo code, a different interleaving compatible with the data length and determined for each protection level should be conducted in addition to the puncturing process [2]. To date, several methods have been suggested mainly for conventional block interleavers, like allocating an exclusive interleaver for each level or a single interleaver for all levels, where the interleaver length is adjusted for different levels. For the block interleaver with a fixed permutation, an interleaver for each level has been proposed in [2], while a circular-shift interleaver for all protection levels usable for the short data lengths is suggested in [3]. In addition, a suitable interleaver for all protection levels has been designed, providing a UEP turbo code without the need for a puncturing process [4].

In contrast to the fixed permutation rule, it is possible to implement interleavers with random permutations for a code with the variable data length. Semi-random interleavers are known as the most efficient interleavers with random permutation. In this type of interleaver, the distance between two adjacent permuted bits should not be less than an allocated value. The best performance of this interleaver with the length L is achieved when the minimum distance is set to the $\lfloor\sqrt{\frac{L}{2}}\rfloor$ value [5]. A structure of the semi-random interleavers usable for permutation of the data blocks with the variable length has been proposed in [6]. The obtained interleaver is named the prunable semi-random interleaver. In this interleaver, a semi-random interleaver according to the shortest data length is designed. Then for the longer lengths, the new required position is randomly inserted. In this interleaver, if after several runs the selected positions do not satisfy the appointed minimum distance, the minimum distance value will be decreased and the above procedure is followed based on the new minimum distance. This reduction degrades the code performance and in order to overcome this problem, a new algorithm has been introduced to apply the semi-random interleaver for different data block lengths, without decreasing the threshold value [7]. Recently, Dioni and Benedetto presented a modification on the prunable interleaver, which improves the code performance with less complexity [8].

The main issue of the interleaver design for the UEP turbo code application is related to the flexibility of adjusting its specifications according to the varying length of data blocks. In contrast to the block interleavers, convolutional interleavers are designed with less complexity and more flexibility to adjust their structures with the length variations of data blocks. Due to the non-block behavior of the convolutional interleaver, turbo codes constructed with these interleavers are analyzed from the continuous performance point of view. The continuous analysis of the turbo code shows that it has a similar performance to the block-wise performance of the code, especially for the constituent RSC codes with the low constraint length value. In order to simplify analysis of the turbo code, convolutional interleavers are designed as block interleavers through the insertion of enough stuff bits at the end of each data block returning the interleaver memories to the zero state. This property makes it possible to utilize conventional iterative decoding techniques applied for the block-wise operation of the turbo code. Based on the application of the convolutional interleaver, three different techniques are presented to design the UEP turbo codes.

In the first technique, only one interleaver for all protection levels is considered. In this technique, different puncturing patterns are applied providing different code rates for the protection levels. In order to improve the turbo code performance, a number of the interleaver lines – which represent the interleaver period value and determine the overall number of stuff bits – should be considered proportional to the data block length. Since the length of protection levels usually differs from each other, the application of an interleaver will not guarantee the provision of a suitable performance for all protection levels.

In the second technique, a single interleaver is allocated for each level of the protection. An interleaver compatible with the longest length of the protection levels is designed. Then based on the interleaver properties, interleavers with the shorter periods relevant to the length of other levels are designed without increasing any complexity in the design. Due to the independent interleavers been designed for each level, this technique has more flexibility to be utilized for applications with high variations of data block lengths.

In addition, since increasing the interleaver period affects the code performance, it is possible to define the new model of UEP by applying interleavers with different periods while the puncturing pattern is kept identical for all levels.

In this paper, performance of the proposed techniques to design the UEP turbo codes is verified. Based on the simulation results, the best suitable model corresponding to the specifications of the protection levels is determined. Our simulations confirm that the first technique is more applicable for protection levels, where data lengths are similar, while the second technique is more reliable for varying data block lengths. The third technique can be utilized when some data parts for a given protection level need more protection than other data parts. The organization of the paper is as follows: Section 2 describes the basic structure of convolutional interleavers and explains their application in the construction of the three techniques to design UEP turbo codes. In Section 3 performance of the 4-state turbo code $(1, \frac{5}{7})$ employing three mentioned techniques is verified based on the maximum-likelihood iterative decoding. Finally, Section 4 concludes the paper.

2. Convolutional interleaver structure

Convolutional interleavers consist of T parallel lines which define their period. Each line of these interleavers have conventionally M memory units more than the previous line, which define the space value parameter of the interleaver. Hence, depending on the distribution of input data to each line of the interleaver, the interleaved input data appear in different time slots at the interleaver output. Figure 1 shows the convolutional interleaver structure with the period $T = 8$ and space value $M = 1$. In order to make isolated interleaved data, some stuff bits are inserted at the end of each input data block returning the memories to the zero state. Then, an optimization is carried out through the deletion of zero stuff bits at the end part of

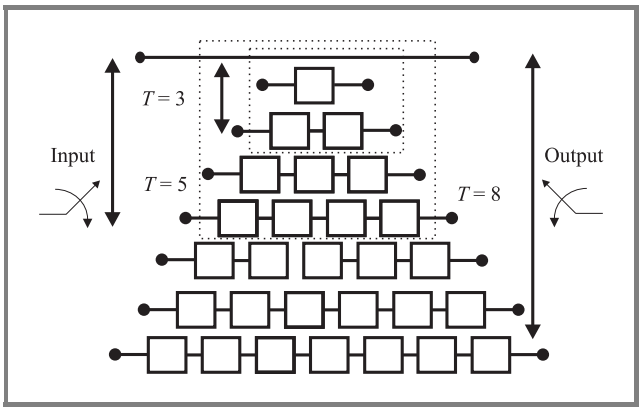


Fig. 1. Consideration of convolutional interleaver $(T = 3,\ M = 1)$ and $(T = 5,\ M = 1)$ from the interleaver $(T = 8,\ M = 1)$.

the interleaved data, reducing the number of stuff bits to the number of the interleaver memories. Figure 2 shows the optimized interleaving procedure for the interleaver $(T = 8,\ M = 1)$ and the length $L = 57$.

The convolutional interleaver with a specific period and space value has the flexibility to interleave data blocks with different lengths. In turbo code applications, when the encoded data blocks, with the variable lengths obtained from an interleaver are punctured with different rates, the UEP turbo codes can be achieved. Conducted simulations of turbo codes with different interleaver lengths indicate that the increment of the data block length, and period of the convolutional interleaver should be increased to provide sufficient performance for the code with a reasonable number of stuff bits [9]. This is more sensitive for an interleaver with a short data block length and leads to a design of an interleaver compatible with the required performance of the code with the longest data block length for the given protection level.

However, since data with the highest protection level require the lower code rate, the data block length is normally considered shorter at this level than at other levels. Hence, designing a convolutional interleaver based on the longest length for all protection levels, increases the number of stuff bits for the levels with shorter lengths and can result in producing the overall number of stuff bits greater than the number of valid data allocated to that level. This is observed when the length variations between different levels is relatively high. Therefore, the convolutional interleaver applied for this type of UEP turbo code is designed based on the shortest block length for all protection levels.

In order to apply an interleaver corresponding to the data specification of each level, it is necessary to employ an independently designed interleaver for each level. It is easily observed that by choosing some lines of an interleaver with the higher period another convolutional interleaver

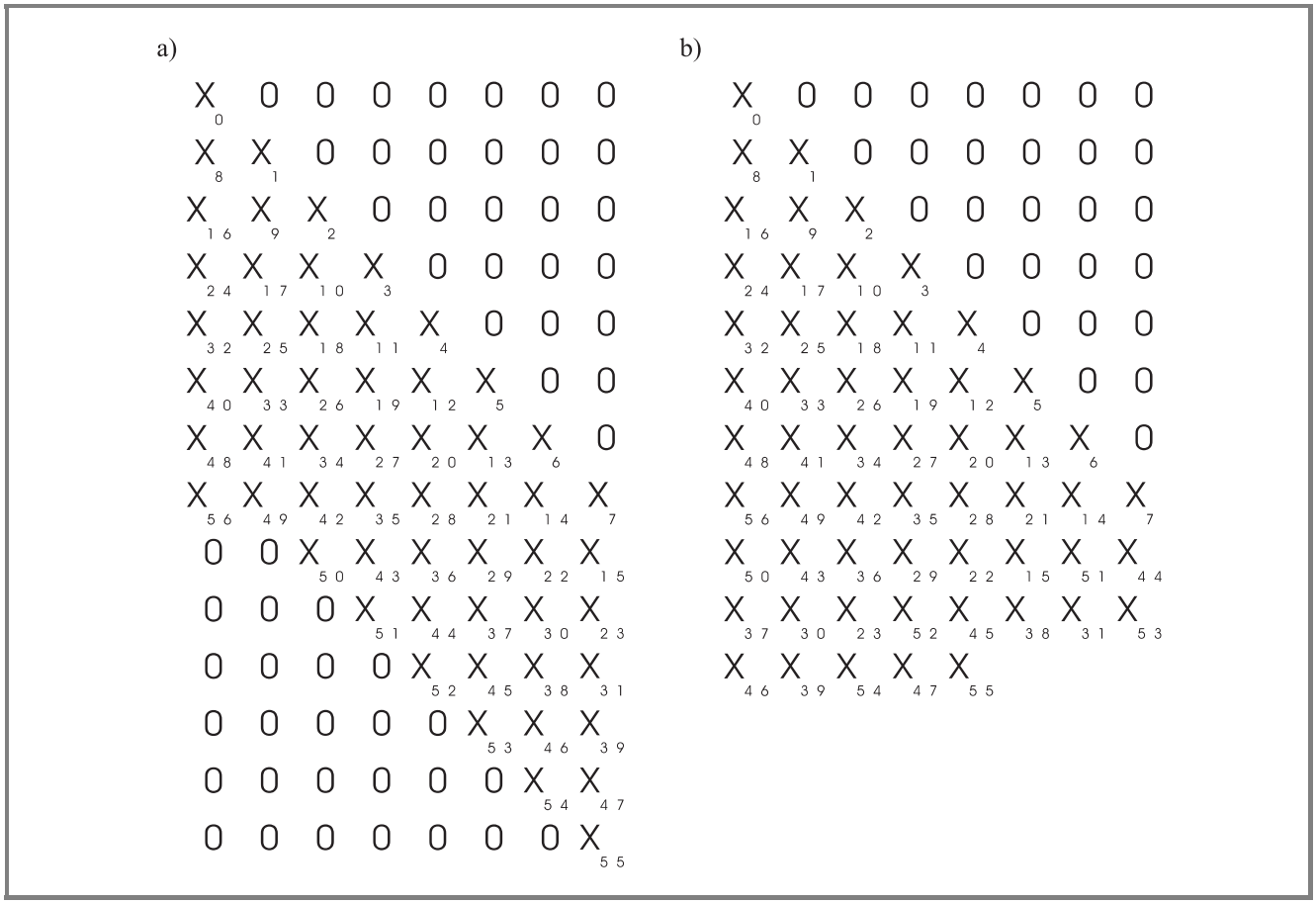


Fig. 2. Interleaved data block with an interleaver $(T = 8,\ M = 1)$ and length $L = 57$: (a) non-zero bit deletion; (b) zero bit deletion.

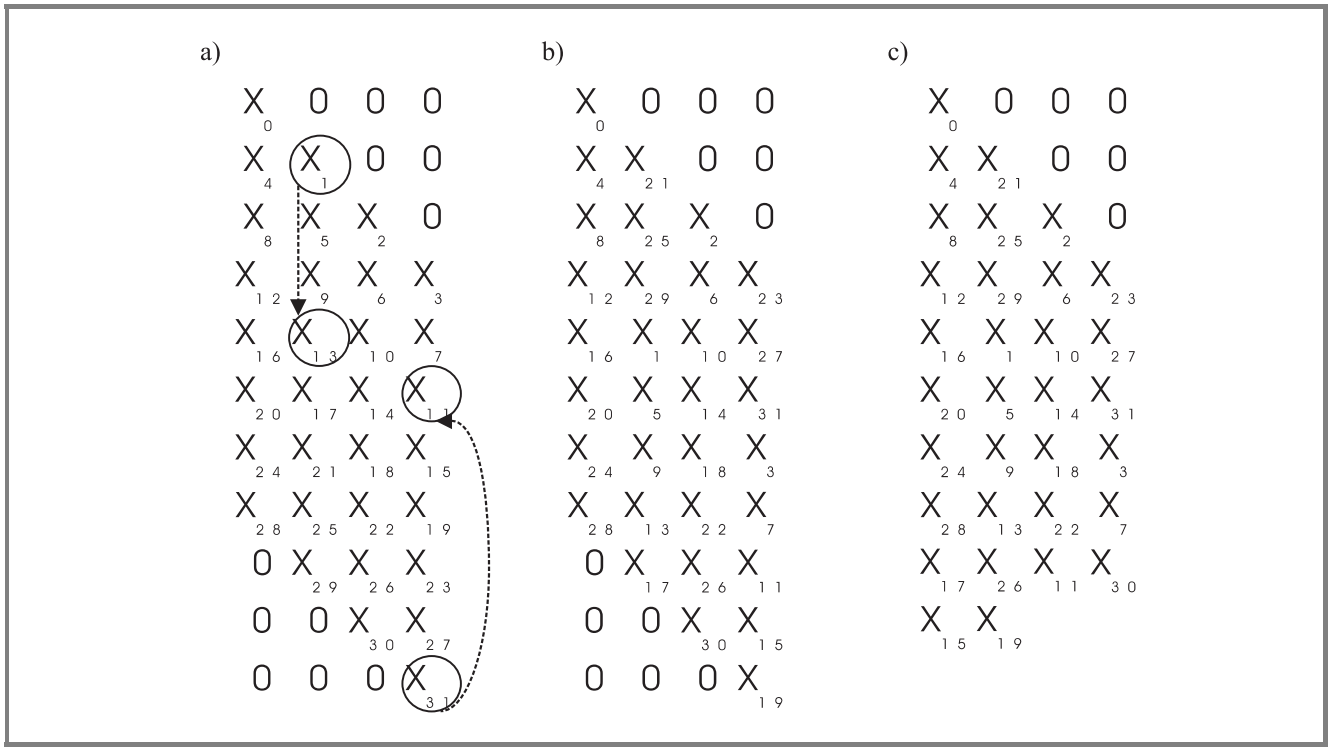


Fig. 3. Modification procedure for the interleaver $(T = 4,\ M = 1)$: (a) interleaved data length $L = 32$; (b) shifted even column bits equal to $3*T$; (c) deletion of zero bits at the end part of the interleaver.

with a shorter period is obtained. For example, Fig. 2 shows that convolutional interleavers $(T = 3,\ M = 1)$ and $(T = 5,\ M = 1)$ can be obtained from the convolutional interleaver $(T = 8,\ M = 1)$ when the relevant input bit streams are distributed to the first 3 and first 5 lines, respectively. These interleavers are created by controlling the distribution of input data blocks to some of the interleaver lines to generate different interleaved data. Interleaved data obtained from different periods are specifically punctured to provide UEP turbo codes. Based on the above observation, many interleavers with shorter periods can be constructed from an original interleaver with a longer period. For simplicity, interleavers with the space value 1 $(M = 1)$ are considered, where the distribution of data always starts from the line without the memory.

Despite applying different puncturing patterns, an interleaver for each level with different periods and a fixed code rate for all levels to provide different protection levels is applied. In this case, for the highest protection level, an interleaver with the longest period is designed such that it produces a reasonable number of stuff bits. Then, based on the order of other protection levels, interleavers with shorter periods are constructed by selecting of some lines of the original interleaver. For example, in Fig. 2, contrasting to the previous technique, the interleaver $(T = 8,\ M = 1)$ is applied for the highest protection level, while the interleavers $(T = 5,\ M = 1)$ and $(T = 3,\ M = 1)$ are used for to the second and third protection levels, respectively.

For each technique, a modification can be performed to the interleavers, improving the code reliability with the lower number of stuff bits. This is generally accomplished by shifting the bits of the interleaved data located at the even columns. Figure 3 shows the modification procedure of the interleaver $(T = 4,\ M = 1)$. First, the input data blocks are regularly interleaved and then the bits located at the even columns are shifted by $3{*}T$ units. Similarly to the proposed modification in [10], the number of shifted bits is considered even. In case of an odd number of bits, the zero stuff bits located on the top of the first bit of even columns are involved in the modification process. Finally, zero stuff bits located at the end part of the interleaved data are deleted to optimize the number of stuff bits.

3. Simulation results

In simulations, convolutional interleavers with short and long data block lengths have been applied for the three mentioned types of UEP with the 4-state tubo code $(1, \frac{5}{7})$. For the code, trellis termination and truncation is utilized in the first and the second RSC encoders, respectively. To reduce the number of stuff bits to be equal to $\frac{T(T-1)M}{2}$, they will be removed from the end part of the systematic and the first parity data, since stuff bits are inserted after trellis termination and do not have any effect on the code performance. For simplicity, the effect of these stuff bits for the systematic and the first parity data are considered getting the exact code rate at each level. At the decoder, the iterative decoding is accomplished and the BER is only calculated based on the length of the original bit stream without stuff bits. Regarding this structure, the code rate of each level is calculated by

$$R_i = \frac{l_i}{n_{\mathbf{P_i}} + n_{\mathbf{Q_i}} + n_{\mathbf{O_i}}}, \tag{1}$$

where l_i, $n_{\mathbf{O_i}}$, $n_{\mathbf{P_i}}$ and $n_{\mathbf{Q_i}}$ denote the length of the puncturing matrix, length of the matrix of 1 s for the systematic data, and number of bit 1 in puncturing matrices of the ith level for the first and second RSC encoder with the length of l_i, respectively. For the short and long data block lengths, 3 and 4 protection levels have been considered, respectively. Tables 1–5 give specifications of puncturing patterns and protection levels of each UEP type.

Table 1
Puncturing patterns for different protection levels

Rate	l	**P**	**Q**	**O**
1/3	1	[1]	[1]	[1]
2/5	2	[1 1]	[1 0]	[1 1]
1/2	2	[1 0]	[0 1]	[1 1]
2/3	4	[1 0 0 0]	[0 0 1 0]	[1 1 1 1]
3/4	6	[1 0 0 0 0 0]	[0 0 0 1 0 0]	[1 1 1 1 1 1]

Table 2
Specifications of 3 protection levels with the fixed interleaver period and different code rates

Level	Length (L')	Interleaver period (T)	Rate (R)
1	32	4	1/3
2	48	4	1/2
3	112	4	2/3
Overall	192	4	$\approx 1/2$

Table 3
Specifications of 3 protection levels with different interleaver periods and code rates

Level	Length (L')	Interleaver period (T)	Rate (R)
1	32	4	1/3
2	48	5	2/5
3	112	6	1/2
Overall	192	5	$\approx 1/2$

Table 4
Specifications of 3 protection levels with different interleaver periods and the fixed code rate

Level	Length (L')	Interleaver period (T)	Rate (R)
1	32	6	1/3
2	48	5	1/3
3	112	4	1/3
Overall	192	4	$\approx 1/3$

Table 5
Specifications of 4 protection levels with different interleaver periods and code rates

Level	Length (L')	Interleaver period (T)	Rate (R)
1	128	7	1/3
2	512	14	1/2
3	1024	20	2/3
4	2432	30	3/4
Overall	4096	25	$\approx 2/3$

In order to compare performance of the protection levels with the equal error protection (EEP) codes, the overall specification of the code should be determined. With the employment of puncturing at each level, the average code rate with l protection levels is determined by [11]

$$R_{av} = \frac{\sum_{i=1}^{l} L_i}{\sum_{i=1}^{l} \frac{L_i}{R_i}}, \tag{2}$$

where $L_i = L'_i + N_i$ denotes the data block length of the ith level after stuff bit insertion, obtained from summation of the original input data block length L'_i and the number of stuff bits N_i. The above protection parameters have been simulated by the soft output Viterbi algorithm (SOVA) [12] with 8 iterations in the presence of additive white Gaussian noise (AWGN). The equivalent interleaver specifications can be determined based on the number of stuff bits or the interleaver periods and the data block lengths for each level. In this case, the equivalent interleaver period for the overall rate is given by

$$T_{av} = \frac{\sum_{i=1}^{l} L_i T_i}{\sum_{i=1}^{l} L_i}, \tag{3}$$

where T_i represents the interleaver period of the ith level.

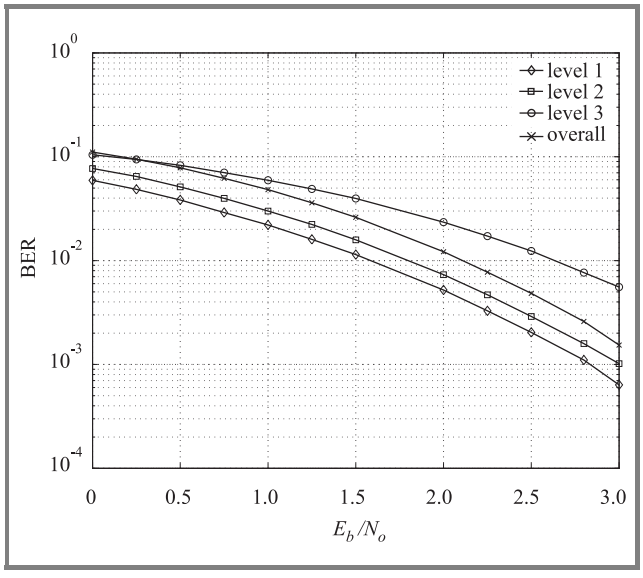


Fig. 4. Unequal error protection for 4-state turbo codes with the fixed interleaver period ($T = 4$) and different rates.

Table 6
Shifted unit values for the even columns bits of the interleaved data of different interleavers

Interleaver period T	4	5	6	7
Shifted unit value	3*T	4*T	4*T	10*T

Figure 4 shows performance of the UEP turbo code based on the fixed interleaver period ($T = 4,\ M = 1$) and the variable code rates of the protection levels. Also, modifications are performed to the interleavers at each level. In the modification process, those shift values which provide better reliability for the code performance are selected. Table 6 gives specification of modifications applied for different interleaver periods. The graphs of Fig. 4 show that levels 1 and 2 are better than the overall performance of the code by 0.5 dB and 0.25 dB, respectively.
Figure 5 illustrates the code performance with different interleavers and code rates applied for protection levels based on the specifications in Table 3. In this figure, level 1 has 0.25 dB better performance than the overall level. When

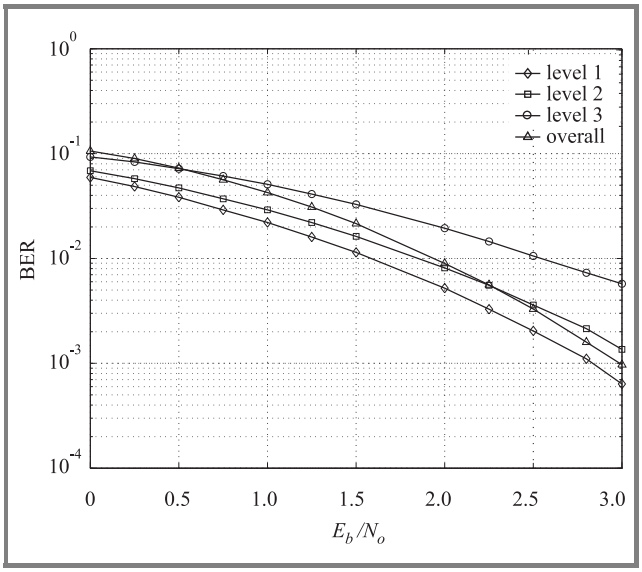


Fig. 5. Unequal error protection for 4-state turbo codes with different interleaver periods and code rates.

the modification is applied to the interleaver[1] of the equivalent EEP for the turbo code, for the overall level, the distance between adjacent bits of the original bit stream increases due to the longer length of every column of the interlever. Therefore a higher weight for the equivalent code with the overall protection level is produced, which consequently improves the code performance at the medium to high signal to noise ratio region.
Figure 6 shows the code performance when different protection is achieved through different interleaver periods with the code rate fixed for all levels. Level 1 has a performance better by 0.5 dB than the overall performance, while

[1]This means that the EEP turbo code has the performance equivalent to the average performance of the considered UEP code.

the level 2 is slightly better than the overall performance. Also, in comparison with the two other methods, level 3 performance has been efficiently improved. Figure 7 shows the performance of the UEP turbo code with four level protection and interleaver length $L = 4096$. In this example, modification is only carried out for level 1. This is accomplished by shifting bits located in the even interleaver lines by $10*T$. In this figure, levels 1 and 2 have 1 and 0.5 dB better performance than the average code performance, while number of stuff bits at these levels has been reduced by 93% and 69.6%, respectively.

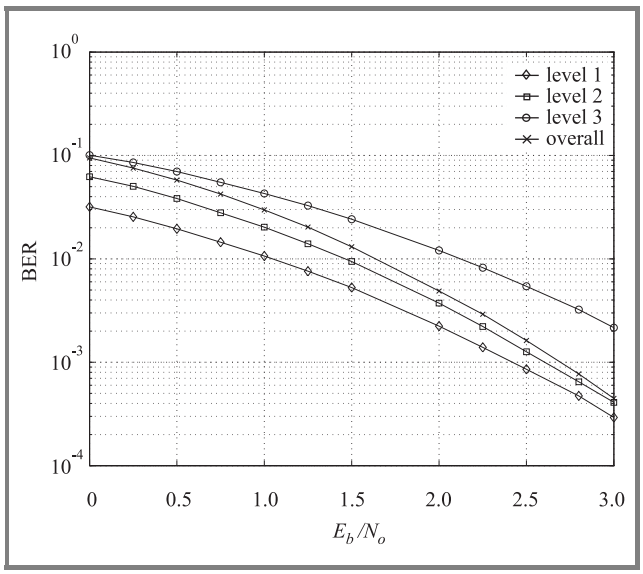


Fig. 6. Unequal error protection for 4-state turbo codes with different interleaver periods and the fixed rate $R = \frac{1}{3}$.

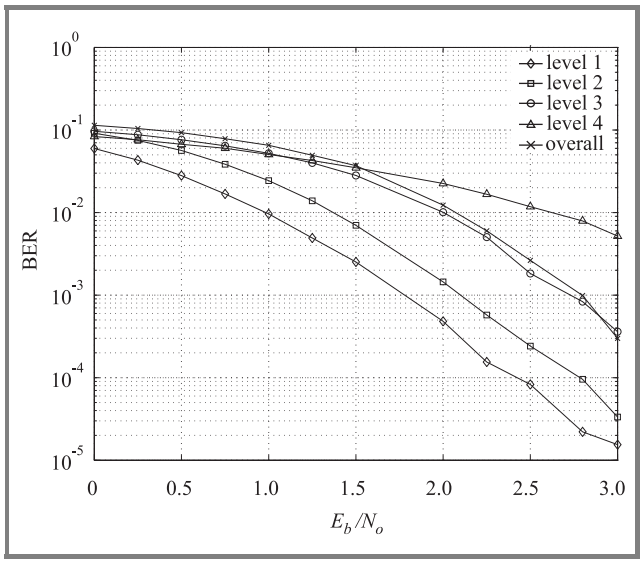


Fig. 7. Unequal error protection for 4-state turbo codes with overall length $L = 4096$.

In addition, level 3 with the lower period and consequently less stuff bits has behavior close to average for the code. However, due to application of the higher code rate and puncturing most of the encoded data, level 4 has the worst performance.

The obtained results from different types of UEP turbo codes indicate that this interleaver has the flexibility to be utilized in UEP turbo code applications with short and long data block lengths. The results represent that the first and third proposed UEP types are useful for the protection levels having similar data block lengths. This is specifically observed for the first type of UEP, when only one interleaver is implemented for all the levels with a lower number of stuff bits and less complexity. However, type 3 improves the performance of every level increasing with and reasonably increases the number of stuff bits.

Comparing the results obtained from the Figs. 5 and 7 indicates that the second suggested technique is more applicable for the cases when the data lengths vary significantly for different protection levels. In such cases, the technique effectively protects the important parts of the data blocks with the shorter periods and lower numbers of stuff bits.

4. Conclusions

In this paper a simple and efficient techniques to design UEP turbo codes with convolutional interleavers was presented. These techniques are implemented based on the interleaver properties and their performance has been examined for the short and long interleaver lengths. The simulation results confirm that the convolutional interleavers have the flexibility to be utilized for different specifications of protection levels. Every technique improves the code performance for the most important parts of data with a shorter period and lower number of stuff bits than the interleaver applied for the EEP turbo codes.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo codes", in *Int. Conf. Commun. ICC*, Geneva, Switzerland, 1993, pp. 1064–1070.

[2] A. S. Barbulescu and S. S. Pietrobon, "Rate compatible turbo codes", *IEE Electron. Lett.*, vol. 31, no. 7, pp. 535–536, 1995.

[3] M. Salah, R. A. Rains, and A. Temple, "A general interleaver for equal and unequal error protections of turbo codes with short frames", in *Int. Conf. Inform. Technol. Cod. Comput. ITCC*, Las Vegas, USA, 2000, pp. 412–415.

[4] M. Grangetto, E. Magli, and G. Olmo, "Embedding unequal error protection into turbo codes", in *35th Asil. Conf. Sig. Syst. Comput.*, Pacific Grove, USA, 2001, vol. 1, pp. 300–304.

[5] S. Dolinar and D. Divsalar, "Weight distributions for turbo codes using random and nonrandom permutations", *TDA Progr. Rep.*, pp. 56–65, 1995.

[6] M. Ferrari, F. Scalise, and S. Bellini, "Prunable s-random interleavers", in *IEEE Int. Conf. Commun. ICC*, New York, USA, 2002, vol. 3, pp. 1711–1715.

[7] P. Popovski, L. Kocarev, and A. Risteski, "Design of flexible-length s-random interleaver for turbo codes", *IEEE Commun. Let.*, vol. 8, no. 7, pp. 461–463, 2004.

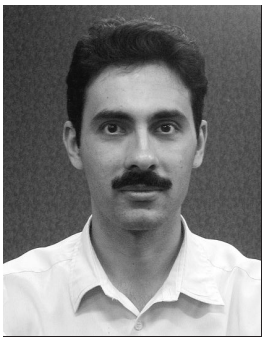
[8] L. Dioni and S. Benedetto, "Design of fast-prunable s-random interleavers", *IEEE Trans. Wirel. Commun.*, vol. 4, pp. 2540–2548, 2005.

[9] S. Vafi and T. Wysocki, "On the performance of turbo codes with convolutional interleavers", in *11th Asia-Pacific Conf. Commun. APCC*, Perth, Australia, 2005, pp. 222–226.

[10] S. Vafi and T. Wysocki, "Modified convolutional interleavers and their performance in turbo codes", in *2nd SympoTIC'04*, Bratislava, Slovakia, 2004, pp. 54–57.

[11] G. Caire and E. Biglieri, "Parallel concatenated codes with unequal error protection", *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 565–567, 1998.

[12] 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, 1996.



Sina Vafi received the B.E. degree in telecommunications engineering from the Khajeh Nasireddin-e Toosi (KNT) University of Technology, Tehran, in 1996 and M.E. in electronics engineering from the Islamic Azad University (South Tehran branch) in 1999. From 1996 to 2002, he was involved in research, design and implementation of digital transmission systems in IRAN Telecommunication Research Centre (ITRC) and Huawei Technologies. Since 2002, he has been studying towards a Ph.D. degree at the University of Wollongong, Australia. His research interests include digital transmission systems, wireless communications and error control coding.
e-mail: sv39@uow.edu.au
University of Wollongong
Northfileds Ave
Wollongong, NSW 2522, Australia

Tadeusz Antoni Wysocki received the M.Sc.E. degree with the highest distinction in telecommunications from the Academy of Technology and Agriculture, Bydgoszcz, Poland, in 1981. In 1984, he received his Ph.D. degree, and in 1990, was awarded a D.Sc. degree (habilitation) in telecommunications from the Warsaw University of Technology. In 1992, Doctor Wysocki moved to Perth, Western Australia to work at Edith Cowan University. He spent the whole 1993 at the University of Hagen, Germany, within the framework of Alexander von Humboldt Research Fellowship. After returning to Australia, he was appointed a Program Leader, Wireless Systems, within Cooperative Research Centre for Broadband Telecommunications and Networking. Since December 1998 he has been working as an Associate Professor at the University of Wollongong, NSW, within the School of Electrical, Computer and Telecommunications Engineering. The main areas of Doctor Wysocki's research interests include: indoor propagation of microwaves, code division multiple access (CDMA), space-time coding and MIMO systems, as well as mobile data protocols including those for ad hoc networks. He is the author or co-author of four books, over 150 research publications and nine patents. He is a Senior Member of IEEE.
wysocki@uow.edu.au
University of Wollongong
Northfileds Ave
Wollongong, NSW 2522, Australia

Paper

An identity-based broadcast encryption scheme for mobile ad hoc networks

Ching Yu Ng, Yi Mu, and Willy Susilo

Abstract— Dynamic ad hoc networks facilitate interconnections between mobile devices without the support of any network infrastructure. In this paper, we propose a secure identity-based ad hoc protocol for mobile devices to construct a group key for a setup of a secure communication network in an efficient way and support dynamic changing of network topology. Unlike group key management protocols proposed previously in the literature, mobile devices can use our protocol to construct the group key by observing the others' identity, like the MAC address, which distinguishes the device from the others. In contrast to other interactive protocols, we only need one broadcast to setup the group key and member removal is also highly efficient. Finally, we discuss the security issues and provide security proofs for our protocol.

Keywords— dynamic mobile ad hoc network, identity-based, non-interactive, secure communication protocol, group key management.

1. Introduction

Many modern computing environments involve dynamic ad hoc networks. Ad hoc networks facilitate interconnections between mobile devices without the need of support for any network infrastructure. When a mobile ad hoc network is formed in an open network environment, all intended and unintended devices can listen and observe the broadcasted communication since wireless signal cannot be hidden underground like wired networks. Security is becoming crucial in this environment. Therefore, the content of the communication must be protected so that only group members in the ad hoc group can obtain the information. Hence, a secure communication protocol and a robust group key management scheme are required to provide strong protection for group communication.

A naive approach to provide a secure communication in this environment is to share a common key, $\mathscr{K}$, among the group members, and this key will be used to encrypt and decrypt each message sent among them. The drawbacks of this approach are as follows:

- This protocol requires prior distribution of $\mathscr{K}$ before the network can be formed, which turns out to be inefficient when the key needs to be updated.
- This protocol does not support the dynamics of the group. When a group member decides to leave the group, the key $\mathscr{K}' \neq \mathscr{K}$ needs to be redistributed among the rest of the group members, which is inefficient.
- It is not possible to create a subgroup within the group, since everyone holds the same key.

Another important issue that needs to be considered in an ad hoc network is the trusted authority (TA). Group members should be able to form their network at anytime because of the mobility of ad hoc network. Hence, we cannot expect an online TA who can always redistribute a key $\mathscr{K}$ whenever needed. A common solution to avoid the need of TA is to employ Diffie-Hellman (DH) key exchange protocol where two parties can come up with the same key $\mathscr{K}$ by exchanging their own random secret interactively and use them to construct the key $\mathscr{K}$ [1]. Although this protocol can only supports two-party, some recent researches have shown that the extension to multiple-party protocol is possible [2–5]. The drawbacks of this approach are as follows:

- The group members must engage in an extensive protocol during the key setup phase. Usually, a leader or a root in the protocol is required to initialize the protocol.
- Depending on the number of group members, the total number of message exchanges can be large when a new key is required (e.g., when a new member joins).
- Due to the large number of message exchanges and the need of leader role, some of the group members may perform more calculations than others (the fairness problem) depending on the key management hierarchy (message exchange order of group members for setting up a new key) being adopted.

This is not encouraged in mobile ad hoc networks, since normally each group member is equipped with a device that has a very limited battery life. Having to perform a huge computation will simply mean that it will drain the battery of the device.

Conceptually, the idea proposed in [6, 7] by incorporating multilinear map may provide a good solution to this key setup problem. In their setting, each group member supplies their own random secret and broadcast it to other group members. Then they can construct a new group key in one round by using the multilinear map computation method. Unfortunately, at this stage, research has not successfully shown that the concrete construction of multilinear map exists. The existing map is the bilinear

map in which Joux showed how to extend the DH key exchange protocol into a tripartite one round version using this map [8]. Barua, Dutta and Sharkar combine the bilinear map with the traditional DH key exchange protocol to construct a tree-based group key management protocol in [9]. Nevertheless, these protocols have not solved the fairness issue mentioned earlier, since some group members still need to perform more computations compared with others.

Having considered the main disadvantages of using key management protocols to setup the group key for mobile ad hoc group, we propose a new protocol which does not require the group members to perform any message exchanges during the generation process of group key. To achieve this goal, we incorporate the identity-based cryptosystem [10] with a bilinear map and pairing computation [11] to replace the contributory setup of a group key as seen in other literature [1–9]. Each group member is treated as a *broadcaster* in which he can select the designated receiver(s)(the whole ad hoc group or part of it) by himself and encrypt the message(key) that is only decipherable by them. Unlike previous protocols, our protocol avoids massive message exchanges for key setup that are sent between group members. Each group member is only required to broadcast one message to setup the group key, and hence, it is most efficient in terms of message exchanges and it provides fairness to every group members. They can also assure that only the designated receiver(s) can decrypt the message(key). We shall note that our protocol is perfect for a small group of people who would like to form a mobile ad hoc network. We would also like to point out that in a mobile ad hoc network, it is not common to have a very large group.

The rest of this paper is organized as follows. In the next section, we will provide some mathematical backgrounds that will be used to construct our scheme. In Section 3, we will provide our proposed scheme follow by a security analysis. Section 4 will conclude the paper.

2. Preliminaries

In this section, we describe the mathematical tools that will be used in our scheme.

2.1. Bilinear map and pairing

Let $\mathbb{G}_1$ be an additive group of points on an elliptic curve and $\mathbb{G}_2$ be a multiplicative group of a finite field. The order of both groups, $|\mathbb{G}_1| = |\mathbb{G}_2| = q$, where q is a large prime and the discrete logarithm problem in $\mathbb{Z}_q^*$ is intractable.

In the following, let P_1, P_2, P, $Q \in \mathbb{G}_1$ be the generators, and $a, b \in \mathbb{Z}_q^*$. A bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a function that:

- is *bilinear*:
  - $\hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab}$,
  - $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q)\hat{e}(P_2, Q)$;
- is *non-degenerate*:
  - for any generator $P \in \mathbb{G}_1$, $\hat{e}(P,P) \neq 1$;
- is *computable*:
  - there exists an efficient algorithm that can compute the map in polynomial time.

A pairing is an efficient algorithm to compute the mapping between $\mathbb{G}_1$ and $\mathbb{G}_2$ for all generators in $\mathbb{G}_1$. Modified Weil pairing is one of the pairings that has been used frequently in recent cryptographic applications [8, 11–13].

2.2. Identity-based cryptosystem

In an identity-based cryptosystem (or ID-based, for short), users are not bound to certificates and no online trusted authorities are required to verify the validity of their certificate. They are bound to their unique identifier (ID) and their private key is obtained from a key generation center (KGC) while their public key is determined with their ID. The center, KGC, can go off-line after the setup of common system parameters and the distribution of keys to users. Later on, one of the two users *Alice* and *Bob*, say *Alice*, wants to send a message to *Bob*, she can encrypt the message using the public key computed from the ID (name, e-mail address, etc., as long as it can be used to uniquely identify the user) of *Bob*. The encrypted message can only be decrypted by *Bob* using his private key previously obtained from the KGC.

Currently the well known ID-based encryption scheme [11] that incorporates the bilinear map and pairing is as follows. The ID-based cryptosystem proposed by Boneh and Franklin:

- `Setup.` KGC generates two groups $(\mathbb{G}_1, +)$ the additive group and $(\mathbb{G}_2, \cdot)$ the multiplicative group both with prime order q together with a bilinear map $\hat{e} : (\mathbb{G}_1, +)^2 \rightarrow (\mathbb{G}_2, \cdot)$. It also selects an arbitrary generator $P \in \mathbb{G}_1$, then picks $s \in \mathbb{Z}_q^*$ randomly and sets $P_{pub} = sP$ as its public key, where s denotes the master secret key. Finally, two cryptographically strong hash functions are selected: $F : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H : \mathbb{G}_2 \rightarrow \{0,1\}^n$, where n denotes the size of the plaintext message space. The system parameters and their descriptions are made public in a tuple $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, n, P, P_{pub}, F, H\}$ while the master secret key s is kept secret.
- `Extract.` After performing physical identification of a user, say *Alice*, and making sure the uniqueness of her ID_{Alice}, KGC generates her secret key as follows. It computes $Q_{\mathrm{ID}_{Alice}} = F(\mathrm{ID}_{Alice})$ and sets $S_{\mathrm{ID}_{Alice}} = sQ_{\mathrm{ID}_{Alice}}$. $S_{\mathrm{ID}_{Alice}}$ is given to Alice as her secret key. It is the same for *Bob* where his identity is ID_{Bob} and his secret key $S_{\mathrm{ID}_{Bob}} = sQ_{\mathrm{ID}_{Bob}}$.
- `Encrypt.` To send an encrypted message to *Bob*, *Alice* first obtains the system parameters and uses *Bob*'s identity to compute $Q_{\mathrm{ID}_{Bob}} = F(\mathrm{ID}_{Bob})$. Then,

to encrypt a message $m \in \{0,1\}^n$, *Alice* picks $r \in Z_q^*$ randomly and computes rP and $g_{\mathrm{ID}_{Bob}} = \hat{e}(Q_{\mathrm{ID}_{Bob}}, P_{pub})^r$. The ciphertext is $C = (rP, m \oplus H(g_{\mathrm{ID}_{Bob}}))$.

- `Decrypt`. Let $C = (U,V)$ be the ciphertext received by *Bob*. To decrypt C using his private key $S_{\mathrm{ID}_{Bob}}$, he computes $g_{\mathrm{ID}_{Bob}} = \hat{e}(S_{\mathrm{ID}_{Bob}}, U) = \hat{e}(sQ_{\mathrm{ID}_{Bob}}, rP) = \hat{e}(Q_{\mathrm{ID}_{Bob}}, sP)^r = \hat{e}(Q_{\mathrm{ID}_{Bob}}, P_{pub})^r$. The message is $m = V \oplus H(g_{\mathrm{ID}_{Bob}})$.

2.3. Single encryption and multiple decryptions

In [14], a new public key based cryptosystem was proposed where there is one public encryption key and multiple decryption keys. It works by considering the polynomial function:

$$f(x) = \prod_{i=1}^{n}(x - x_i) \equiv \sum_{i=0}^{n} a_i x^i,$$

where a_i denotes the coefficient corresponding to x^i after the expansion of $f(x)$, i.e., $a_0 = \prod_{i=1}^{n}(-x_i)$, $a_1 = \sum_{i=1}^{n}\prod_{j\neq i}^{n}(-x_j)$, ..., $a_{n-1} = \sum_{i=1}^{n}(-x_i)$, $a_n = 1$ (note that $f(x_i), 1 \leq i \leq n$ is equal to 0).
Under this construction, any generator $g \in \mathbb{Z}_q^*$ rises to power $f(x)$, i.e., $g^{f(x)}$ *mod* q (q is a large prime) will give the result equals to 1 for $x = x_i$, $i = 1 \ldots n$. (We assume the calculations in this paper are under modulo q and will omit the (mod q) notation in the rest of the paper where it is obvious from the context).
With this property, we let $x_1, x_2, \ldots, x_n$ be the private decryption keys of user $\mathscr{U}_1, \mathscr{U}_2, \ldots, \mathscr{U}_n$, respectively, and $\{g_0, g_1, g_2, \ldots, g_n\} = \{g^{a_0}, g^{a_1}, g^{a_2}, \ldots, g^{a_n}\}$ be the public encryption key tuple. Then a message m can be encrypted as $m \cdot g_0^r$ by choosing a random number $r \in \mathbb{Z}_q^*$ and sending $C = \{m \cdot g_0^r, g_1^r, g_2^r, \ldots, g_n^r\}$ as the ciphertext. The encrypted message can be decrypted by any one of the users by using his own private key x_i to calculate:

$$\begin{aligned} m \cdot g_0^r \cdot \prod_{j=1}^{n} g_j^{r x_i^j} &= m \cdot \prod_{j=0}^{n} g_j^{r x_i^j} \\ &= m \cdot g^{\sum_{j=0}^{n} a_j x_i^j \cdot r} \\ &= m \cdot g^{f(x_i)\cdot r} \\ &= m \cdot 1^r = m. \end{aligned}$$

3. Our proposed scheme

3.1. Security model

3.1.1. System model

In our paper, we consider the situation where a group of users are selected as a subset from the user set $\mathscr{U} = \{\mathscr{U}_1, \mathscr{U}_2, \ldots, \mathscr{U}_k\}$ who would like to form a mobile ad hoc network by using their wireless devices. There exists a key generation center that sets up system parameters, generates and distributes private keys as described in Subsection 2.2. The KGC will accept any person's ID. Upon successful verification of the ID, KGC generates the private key associated with the ID provided. The n users in set $\mathscr{U}$ are those who have contacted the KGC to obtain their private key and have their ID being known by each user within the set. We note that the KGC's role is only to provide the necessary system parameters and distribute each user his private key, hence the KGC is not necessary to keep online after the completion of these procedures and is not required anymore by the users who want to setup a mobile ad hoc network, which fulfill the infrastructureless requirement of dynamic ad hoc networks.

3.1.2. Adversary model

We assume there exists an adversary $\mathscr{A} \notin \mathscr{U}$. All messages available in the network are also available to $\mathscr{A}$. This includes all the messages sent by any set of users $\subset \mathscr{U}$ that wishes to create a mobile ad hoc network. The main goal of $\mathscr{A}$ is to deviate the protocol by decrypting any messages sent within the network intended to any set of users $\subset \mathscr{U}$ but not him. $\mathscr{A}$ is considered to be successful if he wins in the following experiment.
Indistinguishability of encryptions under adaptive chosen plaintext attack (IND-CPA):

1. $\mathscr{A}$ picks a group of user IDs to be attacked and tells the challenger $\mathscr{C}$.
2. $\mathscr{C}$ runs the KGC's `Setup` algorithm to generate the necessary system parameters and his private key. The parameters are given to $\mathscr{A}$ while $\mathscr{C}$ keeps his private key secret.
3. $\mathscr{A}$ can query $\mathscr{C}$ up to q_H hash queries on any ID he wants and up to q_E extraction queries on any ID not equal to the IDs he picked in Step 1. $\mathscr{C}$ will reply with proper hash results on those IDs and runs the `Extract` algorithm to reply $\mathscr{A}$ the private keys he needs.
4. Meanwhile, $\mathscr{A}$ will select two messages $\{m_0, m_1\}$ and gives them to $\mathscr{C}$. $\mathscr{C}$ will then pick one of them randomly by flipping a fair coin to obtain $b \in \{0,1\}$. $\mathscr{C}$ runs the `Encrypt` algorithm on m_b using the IDs picked by $\mathscr{A}$ in Step 1 to get the ciphertext C and gives it back to $\mathscr{A}$ without letting him knows which message is being picked.
5. $\mathscr{A}$ can keep on querying $\mathscr{C}$ the hash or extract values if the total numbers of queries have not exceeded q_H and q_E.
6. Eventually $\mathscr{A}$ will make a guess $b' \in \{0,1\}$ on which message was being picked by $\mathscr{C}$.

If $\mathscr{A}$ somehow managed to guess the correct answer (i.e., $b' = b$) in the experiment on the protocol above then $\mathscr{A}$ wins the experiment and the protocol is not secure. We say that $\mathscr{A}$ has a guessing advantage ε that the probability of $\mathscr{A}$ winning the experiment is $P[b' = b] = \frac{1}{2} + \varepsilon$.

A protocol is said to be secure against IND-CPA if there exist no adversaries with advantage ε that can win the experiment within $q_H + q_E$ queries, in other words ε is negligible.

3.1.3. Security properties

Our protocol is secure against IND-CPA, which means no adversaries can decrypt the messages sent within the network not intended to them. If we consider the messages as some group keys in different sessions, we obtain a secure group key management method with the following properties:

1. *Group key secrecy*. The group key is computationally infeasible to compute.
2. *Known session key secrecy*. Even if one or more previous group session keys are exposed, the current or future session keys are still secure.
3. *Forward secrecy*. If one or more group members' private key are exposed, only the previous session keys are revealed, the current or future session keys are still secure.
4. *Key control secrecy*. The group key is randomly constructed and can not be predicted.

3.2. System construction

Our protocol incorporates the ID-based cryptosystem [10] and its construction using a bilinear map and pairing [11] together with the single encryption and multiple decryption method [14] to create a secure and efficient communication protocol for mobile ad hoc network.

For simplicity, we assume that each of the users $\mathscr{U}_i \in \mathscr{U}$ has contacted the KGC to obtain their ID-based private key $S_{\mathrm{ID}_i} = sF(\mathrm{ID}_i)$. The system parameters $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, n, P, P_{pub}, F, H\}$ are publicly known and each user's ID is known within the user group $\mathscr{U}$. These procedures can be done at anytime before the network is formed.

Let there be a set of users $\mathscr{U}$ and a subset $\mathscr{U}' \subset \mathscr{U}$ of size n wanting to form a mobile ad hoc group. Let $\mathscr{U}_s$ denote a group member who joins $\mathscr{U}'$ and wants to broadcast a message (or session key) to the rest of group. We refer to $\mathscr{U}' \cup \{\mathscr{U}_s\}$ as the current group. Our protocol works as follows:

- `Setup`. Given the system parameters as described above, each of the group members in the current group will perform the following calculations:
  - Select a random number $r \in \mathbb{Z}_q^*$, set $R = rP$.
  - For n other group members in the current group, calculate $e_i = H(\hat{e}(P_{pub}, rF(\mathrm{ID}_i))), i = 1 \ldots n$.
  - Use the e_i values to construct the polynomial function $f(e) = \prod_{i=1}^{n}(e - e_i) = \sum_{i=0}^{n} a_i e^i$.
  - Compute $\{g_0, g_1, \ldots, g_n\} = \{g^{a_0}, g^{a_1}, ..., g^{a_n}\}$.

  After this phase, each group member is equipped with a different encryption key tuple $\{g_0, g_1, \ldots, g_n, R\}$. This tuple will not change throughout the whole session as long as the group topology does not change and none of the private keys of current group members has been exposed.
- `Encrypt`. Let m be the message (or new session key). $\mathscr{U}_s$ will perform the following calculations to encrypt m and broadcast it to the rest of current group members:
  - Select two random numbers $k_1, k_2 \in \mathbb{Z}_q^*$.
  - Raise each component in the encryption tuple to power k_2, i.e., calculate $\{g_0^{k_2}, g_1^{k_2}, \ldots, g_n^{k_2}\}$.
  - Encrypt the message m as $Z = m \oplus k_1$ and compute $A = k_1 \cdot g_0^{k_2}$.
  - Broadcast $C = \{Z, A, g_1^{k_2}, \ldots, g_n^{k_2}, R\}$.
- `Decrypt`. Upon receiving the broadcast message from $\mathscr{U}_s$, each user in current group can decrypt the message with the following calculations:
  - Compute $e_i = H(\hat{e}(R, S_{\mathrm{ID}_i}))$ using his private key S_{ID_i}.
  - Compute $k = A \cdot \prod_{j=1}^{n} g_j^{k_2 \cdot e_i^j}$.
  - $m = Z \oplus k$.

  Note that the computation $H(\hat{e}(R, S_{\mathrm{ID}_i})) = H(\hat{e}(rP, sF(\mathrm{ID}_i))) = H(\hat{e}(sP, rF(\mathrm{ID}_i))) = H(\hat{e}(P_{pub}, rF(\mathrm{ID}_i)))$ and $A \cdot \prod_{j=1}^{n} g_j^{k_2 \cdot e_i^j} = k_1 \cdot g_0^{k_2} \cdot \prod_{j=1}^{n} g_j^{k_2 \cdot e_i^j} = k_1 \cdot \prod_{j=0}^{n} g_j^{k_2 \cdot e_i^j} = k_1 \cdot g^{k_2 \cdot \sum_{j=0}^{n} a_j e_i^j} = k_1 \cdot g^{f(e_i) \cdot k_2} = k_1 \cdot 1^{k_2} = k_1$ and hence message m can be decrypted correctly.

As the mobile ad hoc user group is dynamic, whenever there is a join or leave of group member, simply add or exclude that member's ID during execution of `Setup` to obtain a new encryption key tuple. Note that the pairing computation for the e_i values can be reused if the new join member is a returning old member, only the encryption key tuple is needed to recalculate. This can save a lot of computation as pairing computations are expensive.

3.3. Security analysis

To prove our protocol is secure against IND-CPA, we first assume that there exists an adversary $\mathscr{A}$ that wins in the indistinguishability experiment described in Subsection 3.1. Then we create a simulator $\mathscr{B}$ that intercepts all the communication between $\mathscr{A}$ and the challenger $\mathscr{C}$, $\mathscr{B}$ is able to modify and forward the communication contents and is transparent to $\mathscr{A}$ and $\mathscr{C}$ making $\mathscr{A}$ see no difference between the simulator $\mathscr{B}$ or the real challenger $\mathscr{C}$. The goal of $\mathscr{B}$ is to make use of $\mathscr{A}$ to solve a cryptographic hard problem. Since the hard problem is known to be unsolvable in polynomial time, the assumption that $\mathscr{A}$ exists leads to

a contradiction and hence our protocol is secure. We first review the cryptographic hard problem that we will use in the proof:

Bilinear decisional Diffie-Hellman problem (BDDHP): given an instance (P, aP, bP, cP, θ), where P is a generator $\in \mathbb{G}_1$, $a, b, c \in \mathbb{Z}_q^*$ are chosen uniformly at random and $\theta \in \mathbb{G}_2$. The goal for an attacker is to decide whether $\theta = \hat{e}(P,P)^{abc}$ within polynomial time. BDDHP is hard with an assumption that there exists no polynomial time algorithm for any attacker to solve BDDHP, such that the probability of success is non-negligible.
We now construct the simulator $\mathscr{B}$ as follows (note that $\mathscr{C}$ can be omitted here as $\mathscr{B}$ has simulated it):

1. $\mathscr{B}$ is given an instance (P, aP, bP, cP, θ) of BDDHP as described above.
2. $\mathscr{A}$ picks a group of user IDs to be attacked and tells $\mathscr{B}$.
3. $\mathscr{B}$ runs the KGC's `Setup` algorithm to generate the necessary system parameters. The parameters $\{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, n, P, P_{pub}, F, H\}$ are modified by $\mathscr{B}$ by setting P_{pub} to cP before giving to $\mathscr{A}$.
4. Whenever $\mathscr{A}$ issues a hash query on ID_i, $\mathscr{B}$ replies with his modified hash function F' using the following method:
   - $\mathscr{B}$ maintains a query list $F_{list} : \{\mathrm{ID}_i, r_i, F'(\mathrm{ID}_i)\}$. When the query on ID_i has been asked before, $\mathscr{B}$ looks up F_{list} to find the matching ID_i and replies with $F'(\mathrm{ID}_i)$.
   - If the query on ID_i has not been asked before, $\mathscr{B}$ first selects a random number $r_i \in \mathbb{Z}_q^*$ and further checks that if ID_i is one of the IDs picked by $\mathscr{A}$ in Step 2. If it is, $\mathscr{B}$ sets $F'(\mathrm{ID}_i) = r_i P + bP$, else $\mathscr{B}$ sets $F'(\mathrm{ID}_i) = r_i P$.
   - $\mathscr{B}$ updates F_{list} with the new entry and replies $\mathscr{A}$ $F'(\mathrm{ID}_i)$.
5. Whenever $\mathscr{A}$ issues an extraction query on ID_i, $\mathscr{B}$ replies with his modified `Extract` algorithm using the following method:
   - If the query on ID_i exists on F_{list}, $\mathscr{B}$ takes the $F'(\mathrm{ID}_i)$ value and replies with $S_{\mathrm{ID}_i} = r_i cP$.
   - Otherwise $\mathscr{B}$ follows the hash query replying method to create a new entry for ID_i first then replies with $S_{\mathrm{ID}_i} = r_i cP$.
   - Note that $\mathscr{A}$ is not allowed to query on the IDs picked in Step 2. For extraction values, hence $F'(\mathrm{ID}_i)$ is always in the form $r_i P$ in F_{list} and $r_i cP = cr_i P = cF'(\mathrm{ID}_i)$, which is a perfect simulation of extraction value (since P_{pub} has been replaced by cP).
6. At the time $\mathscr{A}$ provides two messages $\{m_0, m_1\}$, $\mathscr{B}$ picks one of them randomly to obtain $b \in \{0,1\}$ and looks up F_{list} for the r_i values on the IDs picked by $\mathscr{A}$ in Step 2. $\mathscr{B}$ runs the `Setup` algorithm of our protocol to calculate the e_i values for these IDs by setting $R = aP$ and $e_i = H(\theta \cdot \hat{e}(R, P_{pub})^{r_i})$. With these e_i values, $\mathscr{B}$ runs the `Encrypt` algorithm of our protocol to encrypt the selected message m_b and sends $\mathscr{A}$ the ciphertext.
7. $\mathscr{A}$ can keep on querying if the total numbers of queries have not exceeded q_H and q_E.
8. Eventually $\mathscr{A}$ will make a guess $b' \in \{0,1\}$ on which message was being picked by $\mathscr{B}$.

If the guess from $\mathscr{A}$ is correct (i.e., $b' = b$), then $\mathscr{B}$ knows that $\theta = \hat{e}(P,P)^{abc}$, otherwise $\mathscr{B}$ knows that $\theta \neq \hat{e}(P,P)^{abc}$. This is because the e_i values computed by $\mathscr{B}$ are able to construct a valid ciphertext on m_b.
Note that if $\mathscr{A}$ guesses it correctly, then $e_i = H(\theta \cdot \hat{e}(R, P_{pub})^{r_i}) = H(\hat{e}(P,P)^{abc} \cdot \hat{e}(aP, cP)^{r_i}) = H(\hat{e}(aP, bcP + r_i cP)) = H(\hat{e}(R, cF'(\mathrm{ID}_i))) = H(\hat{e}(R, S_{\mathrm{ID}_i}))$. For the above construction of simulator $\mathscr{B}$, we successfully show that $\mathscr{B}$ can solve the BDDHP using the guess provided by $\mathscr{A}$, which leads to a contradiction that BDDHP is unsolvable. Hence the assumption that $\mathscr{A}$ exists is invalid and our protocol is secure. The other security properties mentioned in Subsection 3.1 are straight froward: our IND-CPA protocol implies the *group key secrecy*. With two random values k_1, k_2 selected every time the new session key is broadcasted, we ensure the *known session key secrecy* and *key control secrecy*. *Forward secrecy* can be provided if the group member who has lost his private key is promptly informed to the group and the other group members can simply exclude his ID from the `Setup` phase.

4. Conclusion

We proposed a new secure communication protocol for mobile ad hoc networks. The protocol offers an efficient setup algorithm, together with an efficient protocol for encrypting and decrypting the message among the ad hoc group. Member joining or removal is also simple and quick. With only one broadcast message, each member in the ad hoc group can obtain a new group session key. The use of ID-based cryptosystem provides an easy way to setup our protocol and to include or exclude designated receivers without interrupting the other group members, which can be an advantage for greater flexibility.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.
[2] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication", in *ACM Conf. Comput. Commun. Secur.*, New Delhi, India, 1996, pp. 31–37.
[3] G. Ateniese, M. Steiner, and G. Tsudik, "New multiparty authentication services and key agreement protocols", *IEEE J. Selec. Areas Commun.*, vol. 18, no. 4, pp. 628–639, 2000.
[4] E. R. Anton and O. C. M. B. Duarte, "Group key establishment in wireless ad hoc networks", in *Worksh. QoS Mob.*, Angra dos Reis, Brazil, 2002.

[5] N. Asokan and P. Ginzboorg, "Key-agreement in ad hoc networks", *Comput. Commun.*, vol. 23, no. 17, pp. 1627–1637, 2000.
[6] D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography", *Cryptol. ePrint Arch.*, Rep. 2002/080, 2002.
[7] H. K. Lee, H. S. Lee, and Y. R. Lee, "Multi-party authenticated key agreement protocols from multilinear forms", *Cryptol. ePrint Arch.*, Rep. 2002/166, 2002.
[8] A. Joux, "A one round protocol for tripartite Diffie-Hellman", in *Algorithmic Number Theory, 4th International Symposium ANTS-IV, Lecture Notes in Computer Science*. Leiden: Springer, 2000, vol. 1838, pp. 385–394.
[9] R. Barua, R. Dutta, and P. Sarkar, "An *n*-party key agreement scheme using bilinear map", *Cryptol. ePrint Arch.*, Rep. 2003/062, 2003.
[10] A. Shamir, "Identity-based cryptosystems and signature schemes", in *Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science*. Santa Barbara: Springer, 1984, vol. 196, pp. 47–53.
[11] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing", in *Advances in Cryptology: Proceedings of CRYPTO'01, Lecture Notes in Computer Science*. Santa Barbara: Springer, 2001, vol. 2139, pp. 213–229.
[12] N. P. Smart, "An identity based authenticated key agreement protocol based on the weil pairing", *Cryptol. ePrint Arch.*, Rep. 2001/111, 2001.
[13] D. Nalla, "ID-based tripartite key agreement with signatures", *Cryptol. ePrint Arch.*, Rep. 2003/144, 2003.
[14] Y. Mu, V. Varadharajan, and K. Q. Nguyen, "Delegated decryption", in *Proceedings of Cryptography and Coding, Lecture Notes in Computer Science*. Cirencester: Springer, 1999, vol. 1746, pp. 258–269.

Ching Yu Ng graduated with the M.Sc. degree in computer science from the School of Engineering at the Hong Kong University of Science and Technology in 2003. He continues his postgraduate studies in computer security as a research student in the Center for Information Security at the University of Wollongong in Australia. His research topics include wireless security, group key agreement protocols for dynamic ad hoc network, broadcast encryption schemes and digital signatures.
e-mail: cyn27@uow.edu.au
School of Information Technology and Computer Science
Faculty of Informatics
University of Wollongong
Wollongong, NSW 2522, Australia

Yi Mu received his Ph.D. from the Australian National University in 1994. He was a Lecturer in the School of Computing and IT at the University of Western Sydney and a Senior Lecturer in the Department of Computing at Macquarie University. He currently is an Associate Professor in the Information Technology and Computer Science, University of Wollongong. His current research interests include network security, computer security, and cryptography. He is a Member of the Editorial Board of "Journal of Universal Computer Science", a Senior Member of the IEEE, and a Member of the IACR.
e-mail: ymu@uow.edu.au
School of Information Technology and Computer Science
Faculty of Informatics
University of Wollongong
Wollongong, NSW 2522, Australia

Willy Susilo received a Ph.D. in computer science from University of Wollongong, Australia. He is currently a Senior Lecturer at the School of Information Technology and Computer Science of the University of Wollongong. He is the Coordinator of Network Security Research Laboratory at the University of Wollongong. His research interests include cryptography, information security, computer security and network security. His main contribution is in the area of digital signature schemes, in particular fail-stop signature schemes and short signature schemes. He has served as a program committee member in a number of international conferences. He is a Member of the IACR.
e-mail: wsusilo@uow.edu.au
School of Information Technology and Computer Science
Faculty of Informatics
University of Wollongong
Wollongong, NSW 2522, Australia

Paper

An adaptive LQG TCP congestion controller for the Internet

Langford B. White and Belinda A. Chiera

Abstract— This paper addresses the problem of congestion control for transmission control protocol (TCP) traffic in the Internet. The method proposed builds on the ideas of TCP Vegas, a true feedback control approach to congestion management of TCP traffic. The new method is based on an adaptive linear quadratic Gaussian (LQG) formulation which uses an extended least squares system identification algorithm combined with optimal LQG control. Simulation experiments indicate that the new technique inherits good equilibrium properties from TCP Vegas, but has much superior transient responses which, the paper argues, is important for good dynamic congestion control.

Keywords— TCP, congestion control, LQG, adaptive control.

1. Introduction

The role of congestion control in today's high speed Internet is critical and arguably one of the most essential aspects of traffic management. A significant component of network congestion stems from the fact that over the past two decades there have been no limiting requirements placed on the entry of users onto the network, whilst a simultaneous exponential increase in Internet utilisation has occurred. The resulting effect is one of high levels of congestion in some parts of the network, providing the impetus to improve network efficiency and throughput [1].

The end-to-end transmission control protocol (TCP) [2], designed specifically to avoid and control network congestion, now carries the vast majority ($> 90\%$) of network traffic making it largely responsible for the stability of the Internet to date. However TCP in its original inception is not necessarily well-suited for more current applications. TCP Reno, the most common TCP variant currently in use, has proven effective although shows a decrease in efficacy when multiple packet lossess occur. TCP NewReno, designed specifically to address this issue, is becoming more widely utilised. TCP Vegas, one of the more recent significant proposals, is known to result in substantial improvements in throughput of up to 70% [3]. Performance issues such as fairness has, of late, led to doubt over the suitability of deploying Vegas in a shared environment, however it has recently been demonstrated that the compatibility of Reno and correctly configured Vegas flows results in an improvement in overall network performance [4].

Most TCP algorithms consist of two complementary phases: slow start and congestion avoidance. In slow start the transmission rate – *congestion window* (*cwnd*), is effectively doubled every round trip time (RTT). Once the network has been sufficiently saturated with packets from the source, TCP's congestion avoidance mechanism is invoked. At this point, *cwnd* is conservatively increased so as to gently probe the network until congestion occurs. Reno is what is known as a reactive scheme in that it reacts once congestion has already occurred. TCP Vegas however, is a proactive scheme as it monitors the difference between actual and expected transmission rates and adjusts its *cwnd* accordingly. While Vegas does not further attempt to use any type of model of the relationship between *cwnd* and the measured RTTs, it is clear that there is, at least in principle, the presence of a simple feedback control.

Modelling TCP as a feedback control system has been the subject of recent work (see for example [5–11]). In [5], TCP congestion control is modelled by combining the tools of classical control theory and Smith's principle. However co-operation from intermediate network routers is required, thereby invalidating the implementation of current TCP. Other work of note includes the development of an $\mathscr{H}^{\infty}$ controller for congestion control in communications networks with a capacity predictor [9]. Control theoretic approaches have also been applied to the Vegas mathematical model to address the issues of stability and fairness [10] although this analysis also violates the spirit of current TCP by requiring explicit congestion notification from routers on the network, as does the model of [8]. The delay-based congestion controller of [11] observes current TCP implementation by using measurements of *cwnd* and RTT only. However the model extends only so far as to the system identification of TCP using a simple autoregressive exogenous linear system model.

In this paper, we present a proportional control law for TCP congestion avoidance which we call the linear congestion controller (LCC). The LCC is designed to relate measurements of *cwnd* and logarithmically transformed RTTs to overcome in-built limitations of Vegas whilst possessing the same qualitative behaviour at equilibrium. As LCC uses only information readily available at the source, it is an end-to-end algorithm compliant with today's Internet. We design a model suitable for system identification which we translate to the plant parameters where the plant is the Internet as seen by a given TCP source. Since our model is originally affine rather than linear, we address this issue and synthesise an appropriate linear quadratic Gaussian (LQG) controller followed with the derivation of the corresponding predictor algebraic Riccati equations (ARE) and linear quadratic (LQ) cost function. We are then able to give the adaptive control design for the on-line implementation of LCC which we validate via a series of network simulations.

The outline of the paper is as follows. In Section 2, we derive the LCC model for TCP congestion avoidance. In Section 3, we propose a system model for LCC which is originally affine rather than linear; a property we correct in Subsection 3.1 to make the model suitable for LQG design. We then verify the correctness of the linear model with the standard Matlab command `dh2lqg.m` in Section 4. In Section 5, we give, in detail, the adaptive control design for the LQG component of LCC. In Section 6, we run simulations of the on-line behaviour of LCC and Vegas and compare their respective dynamic performance. Finally, we give our conclusions in Section 7.

2. Control systems model for TCP congestion avoidance

For the purposes of designing a congestion controller, we define the network as being characterised by a set of Q TCP sources $S = \{s_i : i = 1, \ldots, Q\}$ and associated receivers. Each source s_i sets its transmission rate by maintaining a congestion window of length w_i and measures the round trip time r_i (RTT) of a packet, where the RTT denotes the time between the source having sent the packet and the receipt of an acknowledgement caused by its arrival at the receiver. For the sake of clarity, we now drop the i subscript in the following derivation and present a sufficiently generic methodology applicable at each source.

The TCP Vegas [3] congestion avoidance algorithm has the update form for congestion window size (in segments) at synchronous clock time k (with sample period T_s) given by

$$w(k+1) = w(k) + \begin{cases} r(k)^{-1} & \tilde{\varepsilon}(k) > \alpha \\ -r(k)^{-1} & \tilde{\varepsilon}(k) < \beta \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

where

$$\tilde{\varepsilon}(k) = w(k)\left(\frac{1}{\delta} - \frac{1}{r(k)}\right) \tag{2}$$

and $w(k)$ is the congestion window at time instant k, $r(k)$ the current RTT measurement in sample periods, δ the fixed round trip propagation delay and α, β are throughput parameters. Specifically, α and β are threshold values set at the source which serve as estimates for an under-utilised and over-utilised network, respectively. Here we consider the simplified case and assume $\alpha = \beta$ as also considered in [7].

Thus Eq. (1) becomes

$$w(k+1) = w(k) + \frac{\text{sign}[e(k)]}{r(k)}\ , \tag{3}$$

where the error signal is given by

$$e(k) = t - w(k)\left(1 - \frac{\delta}{r(k)}\right)\ . \tag{4}$$

Here t is the target number of queued segments. The motivation for this form of error signal stems from the desire to have a specified number of segments queued in the system in order to rapidly take up any bandwidth which becomes available. By definition, $w(k)$ is the number of (unacknowledged) segments, and, the term in parentheses in Eq. (4) is the proportion of those which are queued, rather than in transit. Thus the error signal $e(k)$ in Eq. (4) describes a simple feedback control mechanism.

The quantisation imposed on $w(k)$ by the sign() function in Eq. (3) has been observed to limit the effectiveness of Vegas [12]. We propose replacing Eq. (3) with the proportional control form

$$\begin{aligned} u(k) &= K(z)\, y(k), \\ \varepsilon(k) &= \frac{t}{w(k)\left(1 - \frac{\delta}{r(k)}\right)}, \end{aligned} \tag{5}$$

where $u(k) = \log w(k)$, $K(z)$ is a stable, strictly causal transfer function and

$$y(k) = \log\left(1 - \frac{\delta}{r(k)}\right) \tag{6}$$

is the transformed system output. Setting $s = \log t$ and $z(k) = \log \varepsilon(k)$ we have the linear congestion controller $u(k)$ with error term $z(k)$:

$$\begin{aligned} u(k) &= K(z)\, y(k), \\ z(k) &= s - u(k) - y(k). \end{aligned} \tag{7}$$

Comparing the Vegas error term $e(k)$ and the quantity $z(k)$ we observe $e(k) = 0$ if and only if $z(k) = 0$, meaning the equilibrium values of the Vegas controller Eq. (4) and LCC Eq. (7) are identical. Further, $e(k) > 0$ (respectively < 0) if and only if $z(k) > 0$ (respectively < 0), so the control action results in identical qualitative behaviour. Thus *cwnd* is increased when the estimated number of queued segments is less than the target, and decreased when the number of segments is greater than the target. The key difference is that we have removed the quantisation imposed by the sign() function in Eq. (3) and replaced it with a proportional control. Note that although the Vegas controller does not use a model of the system (the Internet TCP layer viewed by a single user), the limitation of the gain imposed on Eq. (3) by the one-bit quantisation of the error aids in ensuring the stability of the resulting closed loop system. In the next section, we shall generalise the control approach and incorporate a model relating $y(k)$ and $u(k)$.

3. Linear system model and LQG control

We propose an ARMAX type model relating the output signal (transformed RTTs) to the input signal (transformed *cwnd*), that is $y(k)$, $u(k)$, respectively,

$$y(k) = G(z)\ u(k) + H(z)\ \xi(k)\ , \tag{8}$$

where $G(z)$ is a strictly proper ($1 \le M \le N$) stable rational transfer function:

$$G(z) = \frac{\sum_{m=1}^{M} b_m\, z^{-m}}{1+\sum_{n=1}^{N} a_n z^{-n}} = \frac{\sum_{m=1}^{M} b_m\, z^{N-m}}{z^N+\sum_{n=1}^{N} a_n z^{N-n}}, \qquad (9)$$

and $H(z)$ is a stable rational transfer function with stable inverse

$$H(z) = \frac{1+\sum_{p=1}^{P} d_p\, z^{-p}}{1+\sum_{p=1}^{P} c_p z^{-p}} = \frac{z^P+\sum_{p=1}^{P} d_p\, z^{P-p}}{z^P+\sum_{np1}^{P} c_p z^{P-p}}\ . \qquad (10)$$

The signal $\xi(k)$ is a Gaussian white noise process with unknown mean μ and unit variance representing the unmeasured effect of all background traffic on the (transformed) RTTs as observed by the modelled user.
Writing Eq. (8) in canonical state-space form gives

$$\begin{aligned} X(k+1) &= A\ X(k)+B_2\ u(k)+B_1\ \xi(k)\ , \\ y(k) &= C_2\ X(k)+D_{21}\ \xi(k)\ , \end{aligned} \qquad (11)$$

with error equation

$$z(k) = s+D_{12}\ u(k)+C_1\ X(k)+D_{11}\ \xi(k)\ , \qquad (12)$$

where $D_{12} = -1$, $C_1 = -C_2$, and $D_{11} = -\sigma$, and

$$A = \left[\begin{array}{cccc|cccc} -a_1 & -a_2 & \cdots & -a_N & 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & & \vdots \\ 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & -c_1 & -c_2 & \cdots & -c_P \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & 0 \end{array}\right],$$

$$B_2 = \left[\begin{array}{c} 1 \\ 0 \\ \vdots \\ 0 \\ \hline 0 \\ \vdots \\ 0 \end{array}\right], \qquad B_1 = \left[\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \\ \hline \sigma \\ \vdots \\ 0 \end{array}\right],$$

$$C_2 = \left[\begin{array}{cccc|cccc} b_1 & \cdots & b_M & 0 & \cdots & 0 & d_1-c_1 & \cdots & d_P-c_P \end{array}\right],$$

and $D_{21} = \sigma$, where σ^2 represents the variance of the noise $H(z)\xi(k)$. We thus have the system in the usual 4 block form as used by Matlab's `dh2lqg` function with $D_{22} = 0$.

3.1. Removal of constant values

In the above formulation, we have an affine system rather than linear because of the presence of the non-zero mean noise $\xi(k)$ and the set point s which is non-zero in general. The standard LQG design procedure assumes that all signals are zero mean, so that the resulting controller is linear in nature. Thus we need to modify our model to meet this requirement and then synthesise an appropriate affine controller to ensure that the steady state behaviour is suitable.
Using a symbol ˜ to designate quantities which have had their constant parts removed, we can write

$$\begin{aligned} \tilde{\xi}(k) &= \xi(k)-\mu, \\ u(k) &= \tilde{u}(k)+u_\infty. \end{aligned}$$

Next we consider the steady-state error signal

$$z_\infty = c-y_\infty-u_\infty \qquad (13)$$

which must be zero, otherwise we could reduce its mean square value by subtracting its mean. Thus in implementing our control, we should subtract y_∞ from the measurements $y(k)$, pass this signal to the designed controller, and then add u_∞ to the controller output before closing the loop.

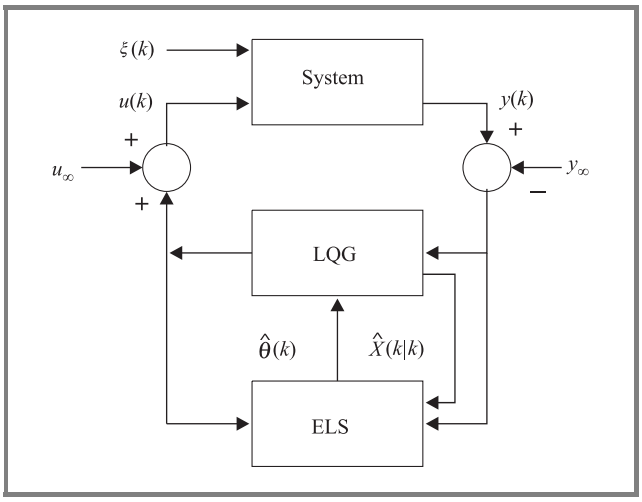


Fig. 1. Adaptive control model.

This process is illustrated in Fig. 1. The design model is now

$$\begin{aligned} X(k+1) &= A\ X(k)+B_2\ \tilde{u}(k)+B_1\ \tilde{\xi}(k), \\ \tilde{y}(k) &= C_2\ X(k)+D_{21}\ \tilde{\xi}(k), \\ \tilde{z}(k) &= D_{12}\ \tilde{u}(k)+C_1\ X(k)+D_{11}\ \tilde{\xi}(k)\ . \end{aligned} \qquad (14)$$

The control design yields the LQG controller $K(z)$ and the control signal is generated according to

$$u(k) = u_\infty+K(z)\,(y(k)-y_\infty)\ . \qquad (15)$$

4. Rapprochement with LQG design tools

To verify the correctness of the Matlab command `dh2lqg.m`, we consider the direct design using control and predictor algebraic Riccati equations (ARE). The LQ part for zero mean signals ($s = 0$) yields a control

$$u(k) = -K_c\ \hat{X}(k|k-1)\ ,$$

where

$$K_c = \left(B_2^T X B_2 + R_c\right)^{-1}\left(B_2^T X A + S_c^T\right)\ .$$

X is the solution to the ARE

$$\begin{aligned} X &= A^T X A - \left(A^T X B_2 + S_c\right)\left(B_2^T X B_2 + R_c\right)^{-1} \\ &\quad \times \left(B_2^T X A + S_c^T\right) + Q_c \end{aligned}$$

and the parameters R_c, S_c and Q_c are the cost matrices in the LQ cost function:

$$J = \mathrm{E}\left\{X(k)^T Q_c X(k) + 2X(k)^T S_c u(k) + u(k)^T R_c u(k)\right\}\ . \tag{16}$$

We minimise cost function $J = \mathrm{E}|z(k)|^2$, where

$$\begin{aligned} J &= \mathrm{E}\left\{X(k)^T C_1^T C_1 X(k) + 2X(k)^T C_1^T D_{12} u(k)\right. \\ &\quad \left. + u(k)^T D_{12}^T D_{12} u(k)\right\}\ . \end{aligned} \tag{17}$$

Thus minimum error variance control is achieved by setting

$$\begin{aligned} Q_c &= C_1^T C_1\,, \\ S_c &= C_1^T D_{12}\,, \\ R_c &= D_{12}^T D_{12}. \end{aligned} \tag{18}$$

To incorporate a control penalty, we use $R_c = D_{12}^T D_{12} + r$ for some positive quantity r.
The one-step predictions $\hat{X}(k|k-1)$ are produced by a Kalman predictor of the form

$$\hat{X}(k+1|k) = \left(A - K_f C_2\right)\hat{X}(k|k-1) + K_f\ y(k) + B_2\ u(k)\ , \tag{19}$$

where

$$K_f = \left(AYC_2^T + S_o\right)\left(C_2 X C_2^T + R_o\right)^{-1}\ . \tag{20}$$

Y is the solution to the ARE

$$\begin{aligned} Y &= AYA^T - \left(AYC_2^T + S_o\right)\left(C_2 X C_2^T + R_o\right)^{-1} \\ &\quad \times \left(C_2 Y A^T + S_o^T\right) + Q_o \end{aligned} \tag{21}$$

and the noise covariance terms are given by

$$\begin{aligned} Q_o &= B_1\ B_1^T\,, \\ S_o &= B_1\ D_{21}^T\,, \\ R_o &= D_{21}\ D_{21}^T\ . \end{aligned} \tag{22}$$

Substituting from Eq. (4) for $u(k)$, we have the state space description for the LQG controller:

$$\begin{aligned} \hat{X}(k+1|k) &= \left(A - K_f C_2 - B_2 K_c\right)\hat{X}(k|k-1) + K_f y(k)\,, \\ u(k) &= -K_c\ \hat{X}(k|k-1)\,. \end{aligned} \tag{23}$$

It has been verified that the above procedure yields an identical controller to that produced by `dh2lqg.m`.

5. Adaptive control design

Suppose we have measurements $u(k)$ and $y(k)$ for the system in open loop for $k \geq 0$, then we desire to identify the model parameters $a_1, \ldots, a_N$, $b_1, \ldots, b_M$, $c_1, \ldots, c_P$, $d_1, \ldots, d_P$, μ, σ^2 on-line. We firstly address the zero mean case where $s = \mu = 0$. Also, for purposes which will become clear, we remove the noise scaling term (σ) from the model and now assume that the noise process $\xi(k)$ has variance σ^2.
We write the parameter vector θ as

$$\theta = (a_1, \ldots, a_N, b_1, \ldots, b_M, c_1, \ldots, c_P, d_1, \ldots, d_P)^T \tag{24}$$

and let

$$\begin{aligned} \phi(k) &= (y_1(k-1), \ldots, y_1(k-N), u(k-1), \ldots, u(k-M) \\ &\quad , y_2(k-1), \ldots, y_2(k-P), \xi(k-1), \ldots, \xi(k-P))^T\,, \end{aligned}$$

where the observations are given by

$$y(k) = y_1(k) + y_2(k) + \xi(k).$$

Thus we can write

$$y(k) = \phi(k)^T\ \theta(k) + \xi(k)\ . \tag{25}$$

Since y_1 and y_2 cannot be measured separately, we use the extended least-squares (ELS) estimator

$$\begin{aligned} \hat{\phi}(k|k-1) &= \Big(\hat{y}_1(k-1|k-1), \ldots, \hat{y}_1(k-N|k-N), \\ &\quad u(k-1), \ldots, u(k-M), \\ &\quad \hat{y}_2(k-1|k-1), \ldots, \hat{y}_2(k-P|k-P), \\ &\quad \hat{\xi}(k-1|k-1), \ldots, \hat{\xi}(k-P|k-P)\Big)^T, \end{aligned} \tag{26}$$

where

$$\begin{aligned} \hat{y}_1(k-1|k-1) &= C_{21}\hat{X}(k-1|k-1), \\ \hat{y}_2(k-1|k-1) &= C_{22}\hat{X}(k-1|k-1), \\ \hat{\xi}(k-1|k-1) &= y(k-1) - \hat{y}_1(k-1|k-1) \\ &\quad - \hat{y}_2(k-1|k-1) \end{aligned} \tag{27}$$

and $C_{21} = (b_1\ \cdots\ b_M\ 0\ \cdots\ 0 \mid 0)$ and $C_{22} = (0 \mid d_1 - c_1\ \cdots\ d_P - c_P)$.

The parameter estimate is updated using the recursive least squares (RLS) rule:

$$\begin{aligned}\hat{\theta}(k+1) &= \hat{\theta}(k)+G(k)^{-1}\hat{\phi}(k|k-1)\\ &\quad\times\left(y(k)-\hat{\phi}(k|k-1)^T\hat{\theta}(k)\right),\\ G(k+1) &= G(k)+\hat{\phi}(k|k-1)\;\hat{\phi}(k|k-1)^T. \qquad (28)\end{aligned}$$

Thus the identification procedure consists of a Kalman filter (KF) estimating the state $X(k)$ using the current parameter estimates as its model, and an RLS algorithm updating the parameter estimates, using the KF state estimates to construct the regression vector. Figure 1 shows the structure of the adaptive controller.

6. Simulation results

We conducted a series of simulations to compare the behaviour of LCC Eq. (7) and Vegas (as given by Eqs. (3) and (4)). Since the models are control laws for congestion avoidance, we restricted our analysis to this phase of TCP only. We also made the assumption there were no packet losses on the network due to either timeout or the presence of lossy links. Thus having entered congestion avoidance the TCP controller remained in this phase for the duration of the simulation.

The network topology is given in Fig. 2 in which there are two TCP senders and receivers (S_1,R_1), (S_2,R_2) and a third source-sink pair (S_b,R_b) to simulate the aggregate

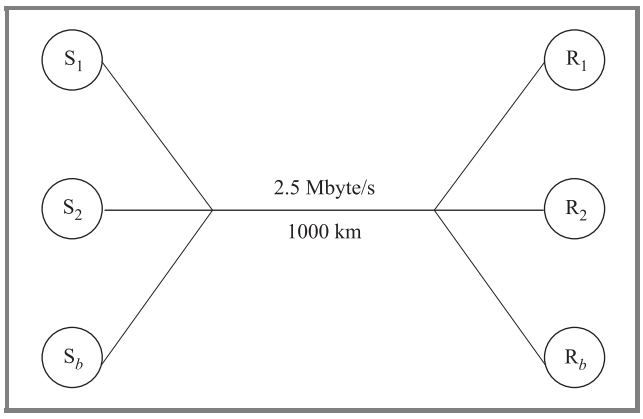


Fig. 2. TCP simulation structure for the two-sender case.

effect of background traffic on the network, generated according to a Poisson distribution. We assumed the presence of a single bottleneck FIFO queue on the network which we used to infer the effects of congestion. We set the network link capacity to 2.5 Mbyte/s and $\delta = 667\ \mu s^{-1}$. The simulation time was 20 s with a sampling rate of 250 samples/s and we staggered the starting time of the sender-receiver pair (S_2,R_2).

Figures 3, 4 and 5 depict the performance of the two models in terms of network link utilisation, the number of times the network queue ran empty and average delay as seen by the two TCP sources. The congestion window target values for S_1 and S_2 were 30 and 80 and the maximum allowed congestion window was 100. Source S_2 commenced sending a quarter-way into the simulation, although it should be noted that the results obtained when starting S_2 half- and then three quarter-way into the simulation are comparable to those given here. For the case where both sources commenced at the same time, the results of LCC were superior to those of Vegas.

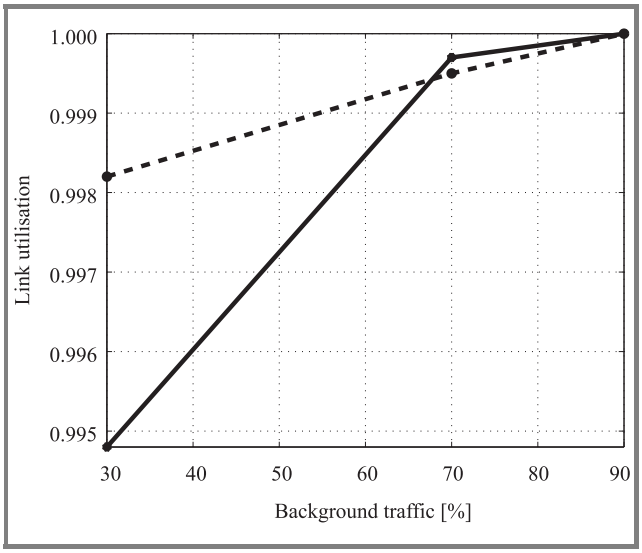


Fig. 3. Network link utilisation of LCC (–) and Vegas (- -). Background traffic loadings are 30, 70 and 90%.

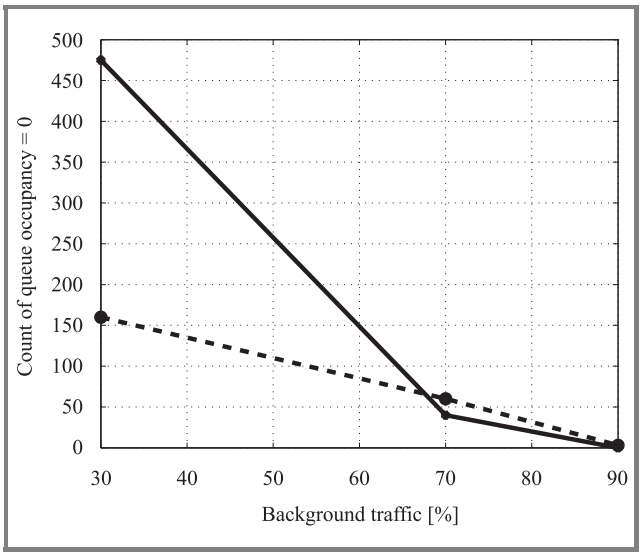


Fig. 4. The number of times the network queue ran empty when running LCC (–) and Vegas (- -). Background traffic loadings are 30, 70 and 90%.

From Figs. 3 and 4 it can be seen that apart from the case of low background traffic (30%), LCC makes better use of the network resources than Vegas. This is particularly true on a more congested network with background traffic

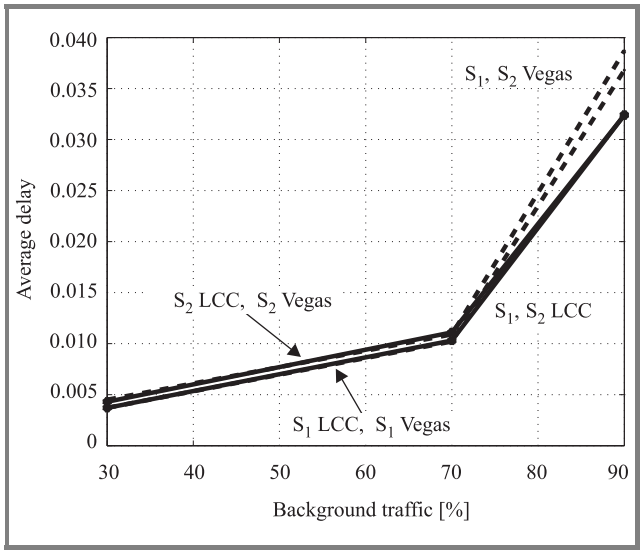


Fig. 5. Average network delay as seen by the two sources when running LCC (–) and Vegas (- -). Background traffic loadings are 30, 70 and 90%.

at 70% and 90%, in which case LCC better utilises the network resources while at the same time reducing the average delay experienced by each of the TCP sources. Moreover, from a snapshot of the congestion window in Figs. 6 and 7

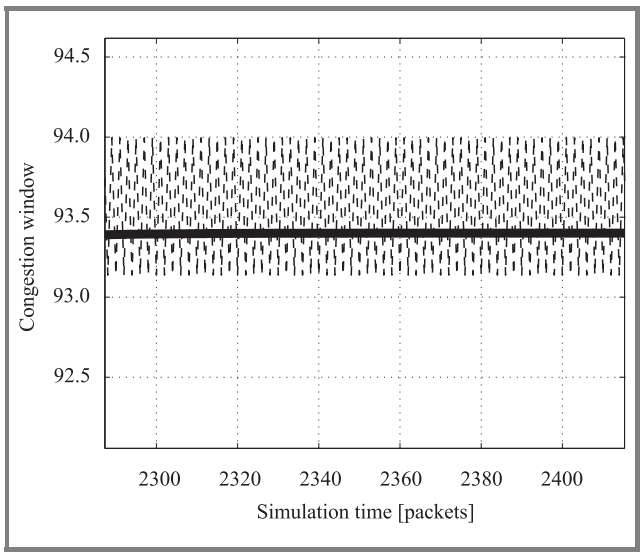


Fig. 6. A close up of the dynamic behaviour of the network measured by the response of the congestion window to S_2 joining the network. The results are for LCC (–) and Vegas (- -) with background traffic at 30%.

as well as the full set of results in Fig. 8, the dynamic behaviour of LCC is more stable than that of Vegas, irrespective of the level of background traffic. In particular, LCC responds more quickly than Vegas to (S_2,R_2) entering the network and becomes relatively stable quite rapidly. In contrast, Vegas takes longer to respond after which time the congestion window oscillates for the remainder of the simulation. This behaviour worsens when the network is more heavily loaded (Fig. 8) in which case the quality of S_1's congestion window is severely compromised. Note also the corresponding controller error as shown in Fig. 9. It can be easily seen that while the S_2 Vegas error eventually stabilises to zero, the S_1 Vegas error is destabilised after S_2 enters the network and continues to oscillate. The LCC controller error rapidly stabilises to zero.

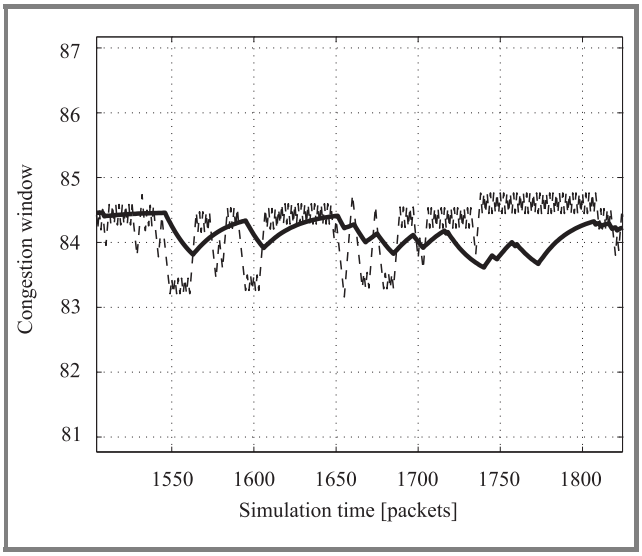


Fig. 7. A close up of the dynamic behaviour of the network measured by the response of the congestion window to S_2 joining the network. The results are for LCC (–) and Vegas (- -) with background traffic at 70%.

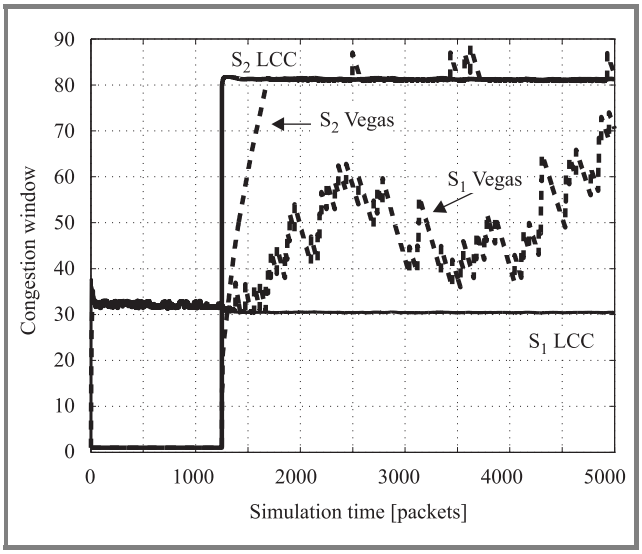


Fig. 8. Dynamic behaviour of the network measured by the response of the congestion window to S_2 joining the network. The results are for LCC (–) and Vegas (- -) with background traffic at 90%.

A secondary issue of importance is that of fairness in the allocation of network resources to the two TCP sources.

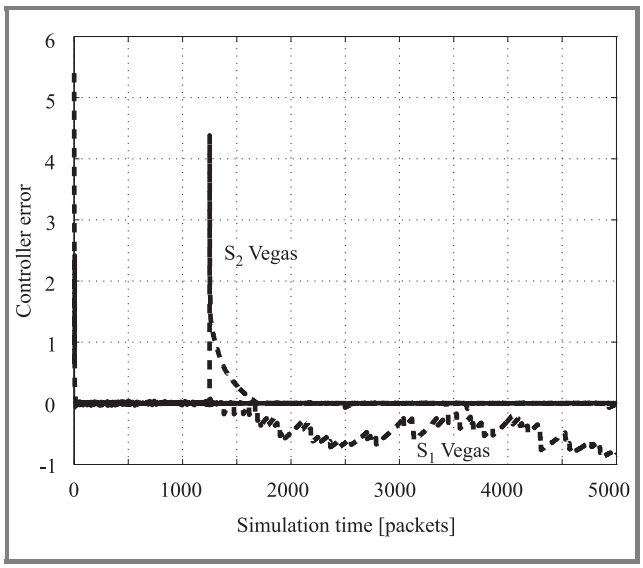


Fig. 9. The controller error of LCC (–) and Vegas (- -). The individual source errors for Vegas are as marked. Background traffic is at 90%.

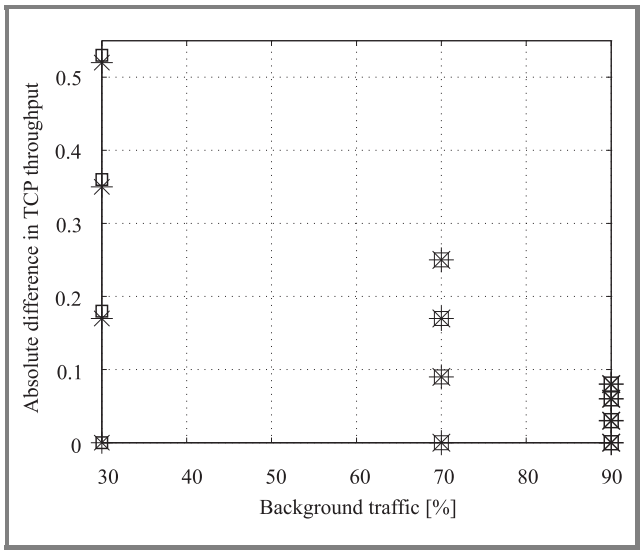


Fig. 10. Absolute difference of throughput experienced by TCP sources S_1 and S_2. The results of LCC are denoted by an asterisk ($*$) and those of Vegas by a square ($\square$). The starting times of S_2 are staggered at each level of background traffic with starts at the same time and then quarter-, half- and three quarter-way through the simulation.

In order to determine the fairness of LCC and Vegas, we set identical target values for sources S_1 and S_2 and staggered S_2's starting times as before, as well as altering network traffic levels. We then computed the absolute difference of the average dynamic throughput of each source, for each controller. The results, given in Fig. 10, show that LCC and Vegas almost entirely identically allocated network resources to both TCP sources S_1 and S_2, which is as expected since it was shown in Section 2 that LCC and Vegas will have the same equilibrium value.

7. Conclusion

In this paper we have described a linear congestion controller for TCP. The proposed controller is based on an adaptive LQG design with extended least squares system identification. A novel transformation of the TCP congestion window size (the control signal) and measured segment round-trip times, was proposed together with an ARMAX type model of the transformed signals. The proposed system design has the same equilibrium behaviour as TCP Vegas, which has been shown to be an improvement over current TCP variants. The proposed controller offers substantially better transient behaviour than TCP Vegas, which we argue is an important factor in practice as there are always TCP users joining and departing the system (Internet) on many different time scales. We have used a bottleneck network queue model to simulate the behaviour of our controller compared to TCP Vegas. Improved transient properties were observed.

In future work we remove the explicit ARMAX model and instead apply modern subspace based LQG approaches. Initial results encourage the use of the subspace-based equivalent [13]. We also present NS-2 based network simulations assuming a fully functioning network in which the simulation is not restricted to the congestion avoidance phase only while also allowing for packet loss. These results will provide a more realistic characterisation of the performance of the new method.

References

[1] V. Firoiu and M. Borden, "A study of active queue management for congestion control", in *Proc. IEEE INFOCOM 2000*, Tel Aviv, Israel, 2000, vol. 3, pp. 1435–1444.

[2] V. Jacobson, "Congestion avoidance and control", in *Proc. SIGCOMM '88*, Stanford, USA, 1988.

[3] L. S. Brakmo and L. L. Peterson, "TCP Vegas: end to end congestion avoidance on a global Internet", *IEEE J. Select. Areas Commun.*, vol. 13, no. 8, pp. 1465–1480, 1995.

[4] W. Feng and S. Vanichpun, "Enabling compatibility between TCP Reno and TCP Vegas", in *Proc. IEEE 2003 Symp. Appl. Internet*, Orlando, USA, 2003, pp. 301–308.

[5] S. Mascolo, "Smith's principle for congestion control in high-speed data networks", *IEEE Trans. Autom. Contr.*, vol. 45, no. 2, pp. 358–364, 2000.

[6] S. H. Low, F. Paganini, and J. C. Doyle, "Internet congestion control", *IEEE Contr. Syst. Mag.*, vol. 22, no. 1, pp. 28–43, 2002.

[7] S. H. Low, L. L. Peterson, and L. Wang, "Understanding Vegas: a duality model", *J. ACM*, vol. 49, no. 2, pp. 207–235, 2002.

[8] Y. Gao and J. C. Hou, "A state feedback control approach to stabilizing queues for ECN-enabled TCP connections", in *IEEE INFOCOM 2003*, San Francisco, USA, 2003.

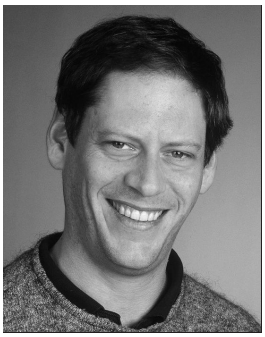
[9] P. F. Quet, S. Ramakrishnan, H. Özbay, and S. Kalyanaraman, "On the $\mathscr{H}^\infty$ controller design for congestion control in communications networks with a capacity predictor", in *Proc. 40th IEEE Conf. Decis. Contr.*, Orlando, USA, 2001.

[10] H. Ohsaki, M. Murata, T. Ushio, and H. Miyahara, "A control theoretical approach to a window-based flow control mechanism with explicit congestion notification", in *Proc. 38th IEEE Conf. Decis. Contr.*, Phoenix, USA, 1999.

[11] H. Ohsaki, M. Morita, and M. Murata, "On modeling round-trip time dynamics of the Internet using system identification", in *Proc. 16th International Conference on Information Networking ICOIN-16, Lecture Notes in Computer Science*. Springer, 2002, vol. 2343, pp. 359–371.

[12] L. B. White and B. A. Chiera, "LQG congestion control for TCP", in *IEEE Worksh. Internet, Telecommun. Sig. Proces.*, Adelaide, Australia, 2004, pp. 70–75.

[13] B. A. Chiera and L. B. White, "A subspace predictive controller for end-to-end tcp congestion control", in *Proc. 6th Austr. Commun. Theory Worksh.*, Brisbane, Australia, 2005, pp. 39–45.



Langford B. White graduated from the University of Queensland, Brisbane, Australia, with the degrees of B.Sc. (maths), B.E. (hons) and Ph.D. (electrical eng.) in 1984, 85 and 89, respectively. From 1986–1999, he worked for the Defence Science and Technology Organisation, Salisbury, South Australia. He received the Australian Telecommunications and Electronics Research Board Prize in 1994 for outstanding young investigator. Since 1999, he has been Professor in the School of Electrical and Electronic Engineering, The University of Adelaide, where he is also Director of the Centre for Internet Research. His research interests include automated planning, signal processing, control, telecommunications and Internet engineering. Professor White is a National ICT Australia Fellow.

e-mail: Lang.White@adelaide.edu.au
Centre for Internet Research (CIR)
School of Electrical and Electronic Engineering
The University of Adelaide
Adelaide, SA 5005, Australia

Belinda A. Chiera graduated from the University of South Australia (Mawson Lakes), Australia, with the degrees of B.App.Sc. (applied mathematics), B.App.Sc. (hons) industrial and applied mathematics and Ph.D. (applied mathematics) in 1993, 1994 and 2000, respectively. From 1999–2001 she was a postdoctoral visitor at The Delft University of Technology, The Netherlands, before returning to Australia to hold research positions at The University of Adelaide and The University of Melbourne. In 2003 Doctor Chiera joined the Centre for Internet Research (CIR) as a research fellow and has since become as a visiting fellow at CIR. Her research interests include telecommunications and internet engineering, networks and protocols, markov decision processes, control theory and signal processing.

e-mail: bchiera@eleceng.adelaide.edu.au
Centre for Internet Research (CIR)
School of Electrical and Electronic Engineering
The University of Adelaide
Adelaide, SA 5005, Australia

Paper

Load-balanced route discovery for mobile ad hoc networks

Mehran Abolhasan, Justin Lipman, and Tadeusz A. Wysocki

Abstract— This paper presents flow-aware routing protocol (FARP), a new routing strategy designed to improve load balancing and scalability in mobile ad hoc networks. FARP is a hop-by-hop routing protocol, which introduces a flow-aware route discovery strategy to reduce the number of control overheads propagating through the network and distributes the flow of data through least congested nodes to balance the network traffic. FARP was implemented in GloMoSim and compared with AODV. To investigate the load distribution capability of FARP new performance metrics were introduced to measure the data packet flow distribution capability of the each routing protocol. The simulation results obtained illustrate that FARP achieves high levels of throughput, reduces the level of control overheads during route discovery and distributes the network load more evenly between nodes when compared to AODV. This paper also describes a number of alternative strategies and improvements for the FARP.

Keywords— ad hoc routing, MANET, load-balancing, on-demand routing, protocols.

1. Introduction

Following the success of 2nd generation mobile (cellular) telephones in the late 1990's, the demand for wireless communication has continued to grow. Part of this success has been due to the growing demand in Internet type application over the wireless medium. This demand has partly been addressed through the introduction of 2.5G GPRS and more recently the 3G (WCDMA1x) networks. Other solutions becoming widely popular are wireless local area networks (also known as Wi-Fi hotspots). Such networks are designed to extend the coverage of wired networks by providing network access to mobile users. One shortcoming of the above technologies is their inability to provide a networking solution in environments where a networking infrastructure does not exists. Currently, infrastructured networks such as 2.5G, 3G and Wi-Fi hotspots exist mainly in metropolitan areas, where consumer demand is high. To address this shortcoming a networking technology is required, which can be easily and cost effectively configured without the need for a pre-existing infrastructure. One such solution is ad hoc networking. In ad hoc networks each end-user node is capable of sending, receiving and routing data packets in a distributed manner. Moreover, such networks can be configured to allow for mobility and perform routing over multiple hops. Such networks are commonly reffered to as mobile ad hoc networks (or MANETs). MANETs are still in their early development stage with the current areas of research spanning across all the levels of the traditional TCP/IP networking model. One interesting area of research in such networks is routing. Designing an efficient routing protocol for MANETs is a non-trivial task. This is primarily due to the dynamic nature of these networks, which requires intelligent strategies that can determine routes with minimum amount of overheads to ensure high levels of scalability. Consequently, researchers have proposed many different types of routing protocols for MANETs. These protocols can be categorised into three groups: proactive, reactive and hybrid routing.

Proactive routing was the first attempt at designing routing protocols for MANETs. The early generation proactive protocols such as DSDV [13] and GSR [4] were based on the traditional distance vector and link state algorithm, which were originally proposed for wired networks. These protocols periodically maintain routes to all nodes with in the network. The disadvantage of these strategies were the lack of their scalability due to exceedingly large amount of overhead they produced. More recent attempts at reducing control overhead in proactive routing can be seen in protocols such as OLSR [7] and TBRPF [3]. These protocols attempt to reduce the control by reducing the number of re-broadcasting nodes in the network.

Reactive (or on-demand) routing protocols attempt to reduce the amount of control overhead disseminated in the network by determining routes to a destination when it is required. This is usually achieved through a two phase route discovery process initiated by a source nodes. The first phase of route discovery starts by the propagation of route request (RREQ) packets through the network. The second phase is initiated when a RREQ packet reaches a node, which has a route to the destination or the destination itself, in which case a route reply (RREP) packet is generated and transimited back to the source node. When the number of flows in the network is low, reactive routing protocols produce significantly lower amount of routing overhead compared to proactive routing protocols. However, for large number of flows reactive protocols experience a significant drop in data throughput. This is because routing control packets are usually flooded (globally) throughout the entire network to find a route to the destination. To reduce the global flooding in the network a number of different strategies have been proposed. In LAR [8] and RDMAR [2] the protocols attempt to use prior location knowledge of the destination to reduce the search zone during route discovery. In LPAR [1] a combination of prior location knowledge and unicasting is used to reduce the number of re-broadcasting nodes within a search zone. In AODV [5] the source nodes use expanding ring search (ERS) to search

nearby nodes first. Therefore, reducing the number of globally propagating control packets.

Hybrid routing protocols combine both reactive and proactive routing characteristics to achieve high levels of scalability. Generally, in hybrid routing protocols, proactive routing is used within a limited region. These regions can be a cluster, a tree or a zone, which may contain a number of end-user nodes. Reactive routing is used to determine routes, which do not lie within a source node's local region. The idea behind this approach to routing is to allow nearby nodes to collaborate and reduce the number of rebroadcasting nodes. Therefore, during a route discovery only a selected group of nodes within the entire network may rebroadcast packets.

While a great deal of attention has been paid to reducing routing overhead, not much attention has been paid in ensuring a fair distribution of traffic flow (or load) between the nodes. Most routing protocols proposed for MANETs select routes based on the shortest-path which is determined using hop count as the route selection metric. This can lead to congestion or the creation of traffic bottlenecks in the network, which can results in higher levels of packets being dropped in the network and rapid depletion of resources in specific nodes. Previous work in designing better load distribution within ad hoc networks includes [6, 10, 15]. These strategies use routing load as the primary route selection criterion. In [11], the author argues that better load distribution can be achieved by flowing data over multiple routes instead of using a single route. In [14], a combination of a delay metric and hop count is used to select routes during the route discovery phase. In this paper, we propose Flow-aware routing protocol (FARP), a routing strategy which aims to reduce the amount of control overhead while ensuring a better distribution of traffic between the nodes. In FARP, a utility metric is introduced to restrict the propagation of route request packet over nodes with minimum number of active data flows from different source nodes. Therefore, congestion or the creation of bottleneck nodes is reduced.

The rest of this paper is organised as follows. In Section 2, we describe FARP. Section 3 illustrates the simulation environment, parameters and metrics used to investigate the performance of FARP with a number of routing protocols. Section 4 presents a discussion of the simulation results. Section 5 points a number of alternative strategies and improvements for FARP and Section 6 gives the conclusions of the paper.

2. Flow-aware routing protocol

The FARP employs the hop-by-hop routing strategy used in AODV. However, unlike AODV, FARP attempts to reduce the amount of control overhead while ensuring a better distribution of data traffic. This is achieved by introducing a flow-aware route discovery strategy, which selects the nodes with the least number of traffic flows.

In FARP, each node maintains a flow table, which stores a $Flow_{ID}$, a flow counter ($Flow_c$) and the ID of the previous node from which the data are received (B_{ID}). The $Flow_{ID}$ is the concatenation of the source, destination ID's of a particular flow and the node of the previous hop, which has forwarded the packet (i.e., $Flow_{ID} = S_{ID}|B_{ID}|D_{ID}$). This strategy allows each node to independently assign the unique flow IDs and identify all data flows travelling through or originating from them. The $Flow_c$ stores the number of different unique data flows that pass through each node. This includes the data flow in which the nodes act as an intermediate node and the data flows that they initiated. Note that the data flow tables maintain information about flows, which are considered as active. To do this, each node updates its data flow counter periodically using timeouts and also reactively when a broken link is reported. Similarly, new flows are added reactively, when a nodes initiates or forwards a data packet which is recorded in the flow table. The following algorithms illustrate the flow-add (FA) algorithm.

Algorithm FA
(∗ The flow-add algorithm ∗)
1. $Flow_t \leftarrow$ flow expiration time
2. $Flow_{ID} \leftarrow$ flow ID for the data packet
3. $Flow_T \leftarrow$ flow table
4. $Flow_c \leftarrow$ flow counter
5. $Flow_A \leftarrow$ flow update flag
6. $S_{ID} \leftarrow$ source node ID
7. $D_{ID} \leftarrow$ destination node ID
8. $B_{ID} \leftarrow$ previous forwarding node ID
9. $Flow_{ID} = S_{ID}|B_{ID}|D_{ID}$
10. $Found \leftarrow$ false a flag used to find flow ID
11. **for** $i \leftarrow 0$, $i < Flow_c$, $i++$
12. **if** $Flow_T[i].Flow_{ID} = Flow_{ID}$
13. $Found \leftarrow True$
14. break
15. **if** $Found = True$
16. Set($Flow_T[i].Flow_t$)
17. **else**
18. $Flow_T[i].Flow_{ID} \leftarrow Flow_{ID}$
19. $Flow_T[i].B_{ID} \leftarrow B_{ID}$
20. Set($Flow_T[i+1].Flow_t$)
21. $Flow_c++$
22. **if** $Flow_c \geq 1$ & $Flow_A != Active$
23. $Flow_A \leftarrow Active$
24. Activate the flow-delete-proactive function

In the FA algorithm, when a node has received or has initiated a data packet, it checks to see if a corresponding $Flow_{ID}$ already exists for that particular flow. If yes, it refreshes the $Flow_t$ for that flow. Otherwise, a new $Flow_{ID}$ is created and a new $Flow_t$ is set. Note that the $Flow_t$ is set by adding the current time by a timeout value[1]. More-

[1]The timeout value can be a constant or a it can be calculated dynamically from the rate at which data packets are received from a particular source.

over, the FA algorithm activates (or re-activates) the flow-delete-proactive (FD_P) function if there are one or more entries in the flow table.

The following algorithms illustrate the FD_P and flow-delete-reactive (FD_R) strategies, respectively.

Algorithm FD_P
(∗ The flow-delete-proactive algorithm ∗)
1. $Time_c \leftarrow$ current time
2. $Flow_T \leftarrow$ the flow table
3. $Flow_c \leftarrow$ flow counter
4. $Flow_t \leftarrow$ flow expiration time
5. $Flow_A \leftarrow$ flow update flag
6. $Total_{Flows} \leftarrow Flow_c$
7. **while** $(Flow_c > 0)$
8. **for** $i \leftarrow 0$, $i < Total_{Flows}$, $i++$
9. **if** $Flow_T[i].Flow_t > Time_c$
10. delete $Flow_T[i]$
11. $Flow_c --$
12. **if** $Flow_c = 0$
13. $Flow_A \leftarrow InActive$

Algorithm FD_R
(∗ The flow-delete-reactive algorithm ∗)
1. $Flow_T \leftarrow$ flow table
2. $B_{ID} \leftarrow$ intermediate node ID in the broken link
3. $Flow_c \leftarrow$ flow counter
4. $Total_{Flows} \leftarrow Flow_c$
5. **for** $i \leftarrow 0$, $i < Total_{Flows}$, $i++$
6. **if** $Flow_T[i].B_{ID} = B_{ID}$
7. delete $Flow_T[i]$
8. $Flow_c --$
9. **if** $Flow_c = 0$
10. $Flow_A \leftarrow InActive$

The FD_P algorithm is used to periodically scan the flow table for expired $Flow_{ID}$s. This is achieved by comparing the flow expiration time (i.e., $Flow_t$) for each $Flow_{ID}$ with the current time. If the $Flow_t$ is greater than $Time_c$, then the flow entries for that particular flow is removed and the $Flow_c$ is decremented. Note that the FD_P function will be deactivated when the $Flow_c$ is set to zero (i.e., when the flow table is empty).

The FD_R algorithm is used to remove flow ID's of the data packets travelling over links which have become inactive. The invalid flow IDs are removed by comparing the ID of the broken link with the ID of the forwarding node (previous hop), then removing the entries in the flow table, which are associated with the broken link. Each time a route entry table is removed, the $Flow_c$ is also decremented. When the flow table scanning phase has been completed, if the flow counter has been set to zero, the flow update flag is set to inactive. This is done to deactive the FD_P function.

When a node has data to send and route to the required destination is not available, then route discovery is initiated. The flow-aware route discovery algorithm is outlined below[2].

Algorithm FSF
(∗ The flow-based selective flooding algorithm ∗)
1. $RREQ_{max} \leftarrow$ maximum number of route request retries
2. $Flow_\tau \leftarrow \tau$ data flow packet threshold
3. $Flow_F \leftarrow$ flow metric
4. $Flow_N \leftarrow 0$ (∗ no metric to be used ∗)
5. $P \leftarrow \{0.125, 0.25, 0.5, 0.75, 1.0\}$ (∗ maximum % of data flow allowed ∗)
6. $RREQ_{max} \leftarrow 4$
7. **for** $i \leftarrow 0$, $i \neq RREQ_{max}$, $i++$
8. $Flow_F \leftarrow Flow_\tau.P_i$
9. **if** $Flow_F = 0$
10. $Flow_F \leftarrow 1$
11. forward_RREQ($Flow_F$)
12. wait for reply
13. **if** $Route = found$
14. break loop
15. initiate data transmission
16. **if** $Route = not\,found$
17. Forward_RREQ($Flow_N$)
18. wait for reply
19. **if** $Route = found$
20. initiate data transmission
21. **else**
22. return route not found

In the FSF algorithm, the source node begins calculating a flow metric ($Flow_F$), which states the maximum number of flows allowed for each node to be able to re-broadcast the RREQ packet. Therefore, each node only re-broadcast a RREQ packet if the number of flows it handles is less than the number speficied in $Flow_F$ (i.e., when $flow_c < Flow_F$). In the FSF algorithm five different levels of data flow (i.e., P) can be selected to calculate the flow metric. During each route request retry, this value is increased until $i = RREQ_{max}$. If the route to the destination is still not found, then source node transmits a RREQ without a flow metric (i.e., $Flow_N$), which allows all intermediate nodes to rebroadcast. If the source node determines more than one route to the required destination, it uses the one with the lowest number of flows and the shortest path. Furthermore, if two routes are found with identical number of flows and hops (which have also least number of flows and hops), then the preferred route is randomly selected.

When a source node has data to send, and a fresh (or active) route already exists or has been determined through a route discovery, then a $Flow_{ID}$ is created and stored, and the data is forwarded to the next hop. Each forwarding node then creates their own flow IDs (as described previously) and continue forwarding the data packets. This process continues (including at the destination node) until the destination node is reached. Furthermore, each consequtive data packet

[2]We refer to this algorithm as flow-based selective flooding (FSF).

is used to update the lifetime of each flow ID (if the flow ID already exists).

To illustrate how FSF algorithm works, assume that $Flow_\tau = 1$ and S1, S2 and S3 (see Fig. 1) want to send data to D1, D2 and D3. Using shortest path (SP) routing,

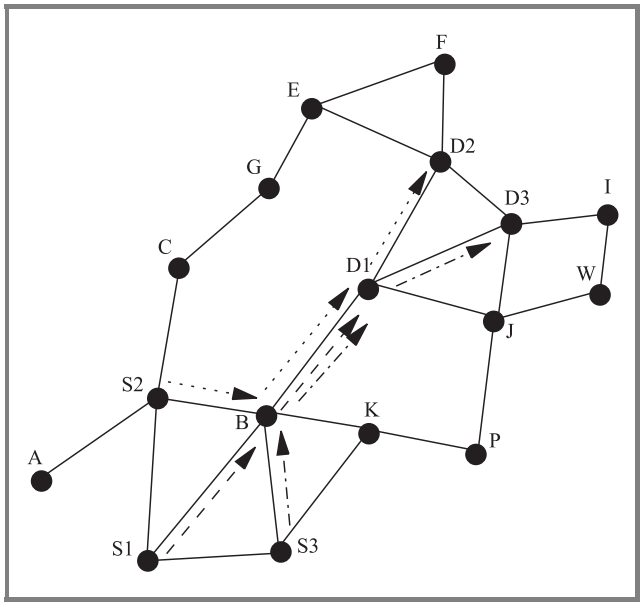


Fig. 1. Data packet flow using SP routing only.

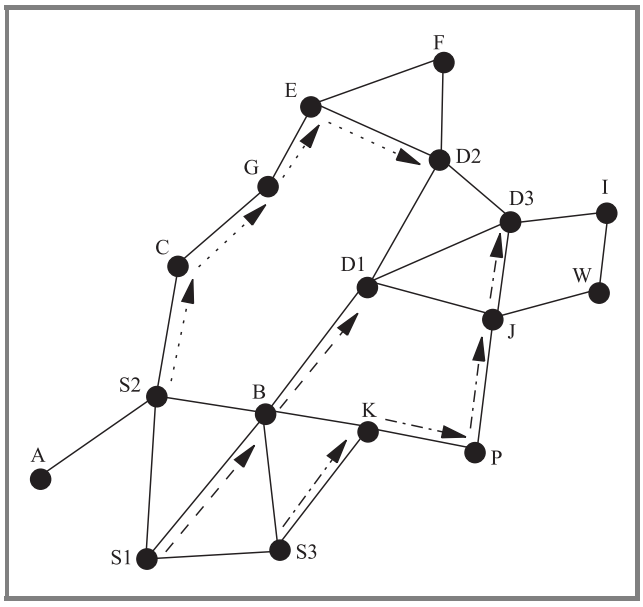


Fig. 2. Data packet flow using FSF.

all data packets travel through node B and D1. Thus creating possible performance bottlenecks at these nodes. In FSF (Fig. 2), the route discovery strategy uses a combination of data flows restriction and SP routing to distribute the packets through nodes C, B and K, instead of through node B only (as was the case in Fig. 1). As a result, FARP ensures a better distribution of data traffic than using purely SP routing.

To illustrate how FARP can reduce the number of control packets, let us assume that S (Fig. 3) wants to send data to D. In this scenario, under SP routing the route discovery

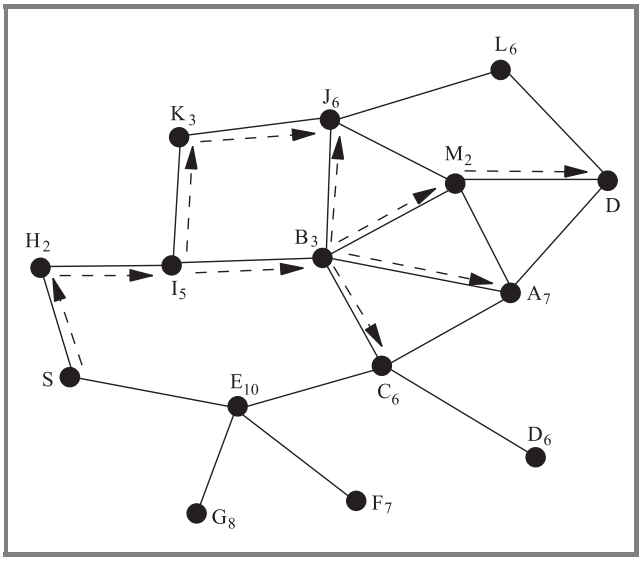


Fig. 3. Illustration of control overhead reduction in FARP (note in X_Z, X represents the node ID and Z is the number of flows).

phase results in transmission of 15 RREQ packets (i.e., all nodes broadcast). However, in FARP, only 6 nodes broadcast the RREQ packet. Thus, a control overhead reduction of 60% is achieved. In scenarios where the number of nodes and traffic level is high, it is expected that FARP will experience significant drop in the number of control packets when compared to other SP-based on-demand routing protocols such as AODV. In Section 4, FARP is compared with AODV using simulation studies performed over densely populated mobile ad hoc network, with multiple number of flows.

3. Simulation model

This section describes the scenarios and parameters used in simulation studies performed for FARP. It also illustrates the performance metrics used to compare FARP with AODV.

3.1. Simulation environment and scenarios

The GloMoSim [9] simulation package was chosen to run the simulations. GloMoSim is an event driven simulation tool designed to carry out large simulations for mobile ad hoc networks. The simulations were performed for 10, 20 and 100 node networks, migrating in a 1000 m $\times$ 1000 m area. IEEE 802.11 DSSS (direct sequence spread spectrum) was used with maximum transmission power of 15 dbm at a 2 Mb/s data rate. In the MAC layer, IEEE 802.11 was used in DCF mode. The radio capture effects were also taken into account. Two-ray path loss characteristics was considered as the propagation model. The antenna height

was set to 1.5 m, the radio receiver threshold was set to –81 dbm and the receiver sensitivity was set to –91 dbm according to the Lucent wavelan card [12]. Random waypoint mobility model was used with the node mobility ranging from 0 to 20 m/s and pause time was set to 0 s for continuous mobility. The simulations ran for 200 s (we kept the simulation time lower due to a very high execution time required for the 40 flow scenario) and each simulation was averaged over eight different simulation runs using different seed values.

Constant bit rate (CBR) traffic was used to establish communication between nodes. Each CBR packet contained 512 bytes and each packet were transmitted at 0.25 s intervals. The simulation was run for 5, 10, 20 and 40 different client/server pairs[3] and each session began at a randomly selected time and was set to last for the duration of the simulation.

Table 1
FARP simulation parameters

Parameters	Values
Flow timeout	3 s
Flow expiration time	2 s
Flow threshold	8
RREQ retry times	6

The FARP routing protocols was implemented on the top of the AODV algorithm. Table 1 illustrates the simulation parameters used for FARP. Note that the flow timeout represents the timeout interval at which the flow table entries are updated. The flow expiration time represents the lifetime of each flow. The flow threshold is used to assume a maximum number of flows at each node. This is used in the FSF algorithm. The RREQ retry times represents the number of times a source can initiate a route discovery before the destination is seen as unreachable.

3.2. Performance metrics

The performance of each routing protocol is compared using the following performance metrics:

- packet delivery ratio (PDR),
- control packet overhead (O/H),
- end-to-end delay,
- total flows per node (TFN).

The PDR is the ratio of the number of number of packets received by the destination to the number of packets sent by the source. Control packet overhead presents the number of control packets transmitted through the network. The end-to-end delay represents the average delay experienced by each packet when travelling from the source to the destination. The TFN represents the total number of data flows handled by each node in the network for the complete duration of the simulation. The above metrics where taken for different values of pause time.

[3]Note that the terms client/server, src/dest and flows are used interchangeably.

4. Results

This section presents the simulation results obtained for FARP and AODV. A performance comparison between both protocols is also provided.

4.1. Packet delivery ratio

Figures 4 and 5 illustrate the PDR results obtained for the 20 and 100 node scenarios. These figures illustrate the packet delivery performance of AODV and FARP in a small to medium size mobile ad hoc network. In the 20 node scenarios both FARP and AODV achieve over 98% PDR. However, in the 100 node scenario it can be seen that FARP achieves a higher level of packet delivery than AODV when node mobility is high (i.e., for short pause times). This is because FARP reduces the probability of establishing

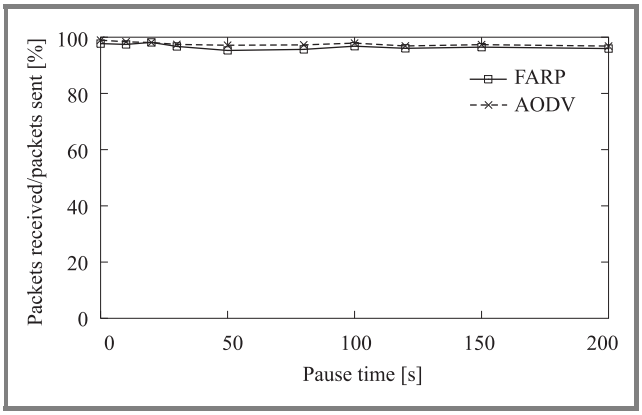


Fig. 4. Packet delivery ratio versus pause time: 20 nodes and 10 flows.

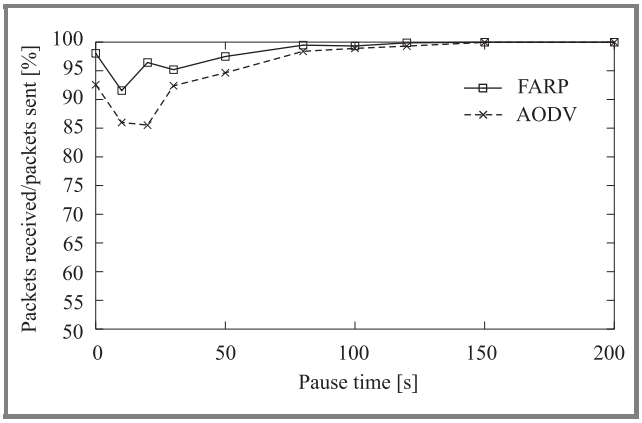


Fig. 5. Packet delivery ratio versus pause time: 100 nodes and 50 flows.

routes over bottleneck (or saturated nodes). Thus in FARP, data packets have a better chance of reaching the required destination than in AODV. Furthermore, FARP introduces a more self-selective approach to flooding than AODV. This means that not every node in the network need rebroadcast control packets. Hence, there is often reduction in channel contention between nodes and smaller chance of packets being lost due to interference and buffer overflows when compared to the blind flooding approach employed in AODV.

4.2. Control packets overhead

Figures 6 and 7 illustrate the number of control packets introduced into the network for the 20 and 100 node scenarios, respectively. In both scenarios it can be seen that FARP produces fewer control packets than AODV. This is

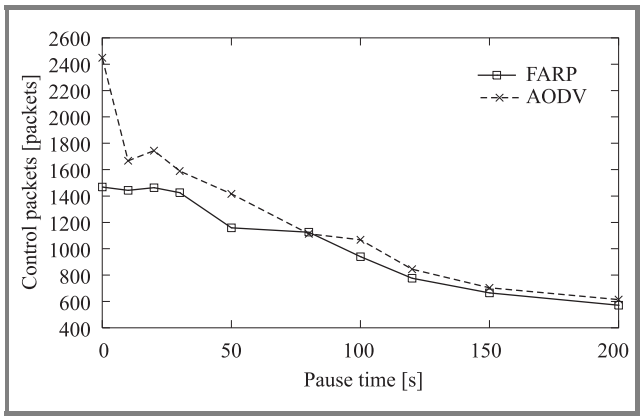


Fig. 6. Control packet overhead versus pause time: 20 nodes and 10 flows.

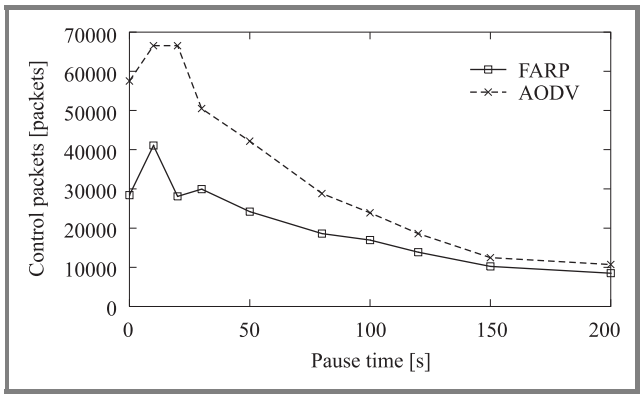


Fig. 7. Control packet overhead versus pause time: 100 nodes and 50 flows.

more evident when mobility is high, because in high mobility both protocols initiate more route discoveries due to more frequent route failures. However, in FARP each route discovery may result in fewer number of control packet rebroadcasts than AODV, due to restriction of flooding over nodes which have fewer flows thereby reducing the number of rebroadcasting nodes when compared with AODV.

4.3. End-to-end delays

Figures 8 and 9 illustrate the end-to-end delay introduced for the 20 and 100 node network scenarios, respectively. In the 20 node scenario, both AODV and FARP produce similar levels of end-to-end delay. This is because

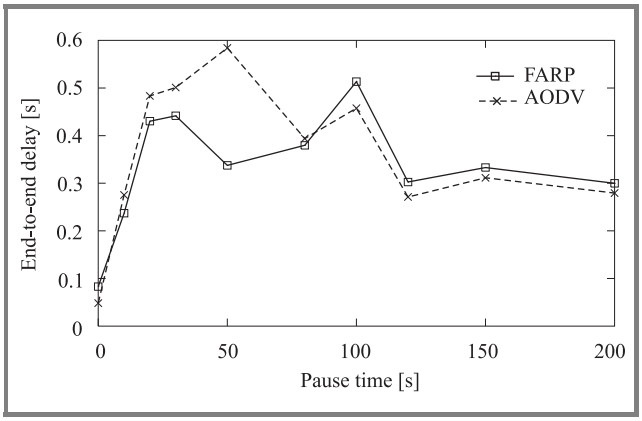


Fig. 8. End-to-end delays versus pause time: 20 nodes and 10 flows.

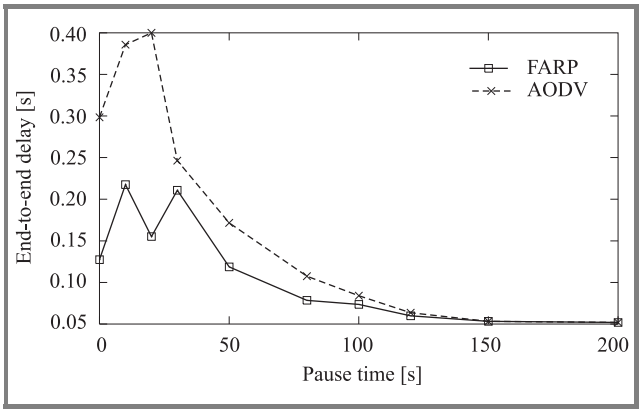


Fig. 9. End-to-end delays versus pause time: 100 nodes and 50 flows.

the amount of traffic introduced into the network is lower than the available bandwidth and the capacity of each node (i.e., no long queue at each node). In the 100 node network with 50 flows, FARP achieves significantly lower end-to-end delay than AODV when mobility is high. This is because AODV produces significantly more control overhead than FARP (as described previously in the control packet overhead results), which increases channel contention between nodes and may increase the time that each data packet spends in buffers before being transmitted.

4.4. Flow distribution

Figures 10, 11 and 12 illustrate the number of different flows handled by each node for zero pause time (i.e., constant node mobility) for the entire duration of the simulation. In the 10 node and 20 node scenario, FARP produces

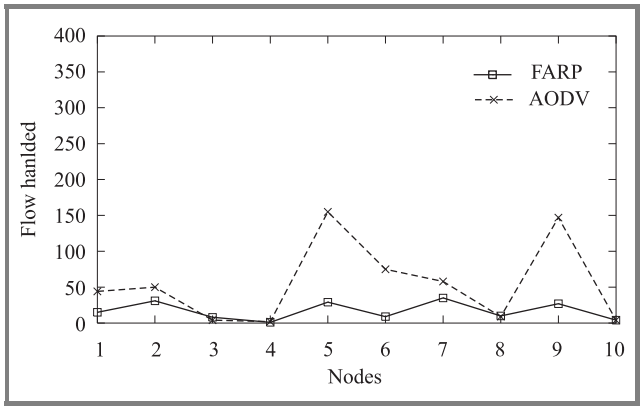


Fig. 10. Flow distribution: 10 nodes and 5 flows.

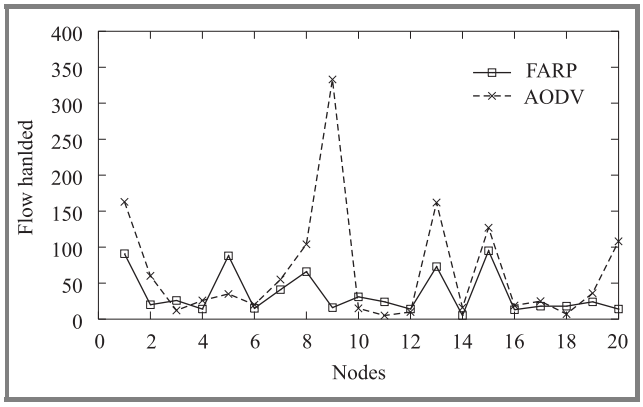


Fig. 11. Flow distribution: 20 nodes and 10 flows.

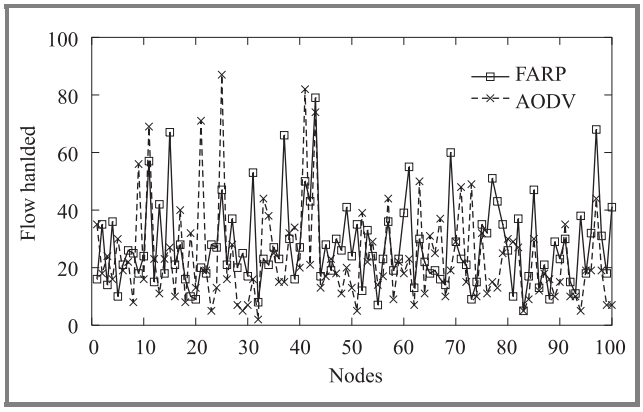


Fig. 12. Flow distribution: 100 nodes and 50 flows.

significantly better flow distribution than AODV. This can be seen by the flatness of the curves. In FARP, the total number of flows at each node varies between 10 to 40 for the 10 node scenario, and 10 to 90 flows for the 20 node scenario. However, in AODV the flows vary between 0 to 150 flows for the 10 node scenario and 0 to 340 flows for the 20 node scenario. Hence, there are larger spikes in the AODV graph than in FARP. This indicates that in FARP flows are more evenly distributed than AODV. In the 100 node scenario, the flow distributions achieved in AODV and FARP are more closely matched than the other less dense scenarios. This is because each node has a higher probability of handling data packets due to the larger traffic density. However, with close observation of the 100 node graph it can be seen that AODV still experiences larger variation in flow distribution. For example, the smallest flow count experienced by a node in AODV is close to 0 flows and the largest is around 90 flows, whereas in FARP the smallest value is close to 8 flows and the largest is close to 78 flows.

5. Alternative strategies and improvements

5.1. Dynamic flow threshold selection

In the FSF algorithm, the flow threshold (the limit for the number of flows allowed at each node) was chosen as a simulation parameter. Therefore, each node in our simulations used a static value for the flow threshold. The disadvantage of a static flow threshold is that it may not always allow for the best flow distribution in the network. To make more accurate prediction of flow limits and better flows distribution, each node must make these decisions dynamically based on the current conditions of the network. One way to calculate the flow threshold dynamically is through the use and exchange of neighbour flow information. In this strategy, each node exchange flow information with their neighbouring nodes (using hello packets) and calculates an average flow per neighbour and the maximum number of flows, which can be experienced by each node at each particular region. Using this information the first few RREQ propagation can be restricted only to the nodes that are handling average or lower levels of flows.

5.2. Rate adaptive flow timeout selection

In our FARP simulations, the flows that are not refreshed every 2 s or less are deleted from the flow table. The disadvantage of this is that different applications may be transmitting data at different rates. Therefore, by assigning a static flow timeout, the flow table may be storing each flow ID for a longer or shorter time than it is required. To overcome this, the flow timeout value can be set by observing the rate at which data packets arrive at each node and assigning a timeout value, which closely matches the expected arrival time.

6. Conclusions

In this paper, we introduced a new routing strategy for mobile ad hoc networks. This routing strategy is referred to as flow aware routing protocol. In FARP, a new route discovery strategy is introduced, which uses the flow information kept at each node to reduce the number of control packets

while ensuring better distribution of data packets between the nodes in the network. This is achieved by restricting the RREQ retransmission over nodes that have the lowest number of flows. We implemented FARP on the top of AODV and compared the performance through simulation. Our results show that FARP reduces the number of control packets transmitted through the network, while achieving improved data flow distribution in the network. In the future, we plan to investigate the performance of FARP over large networks with high levels of mobility.

References

[1] M. Abolhasan, T. A. Wysocki, and E. Dutkiewicz, "LPAR: an adaptive routing strategy for MANETs", *J. Telecommun. Inform. Technol.*, no. 2, pp. 28–37, 2003.

[2] G. Aggelou and R. Tafazolli, "RDMAR: a bandwidth-efficient routing protocol for mobile ad hoc networks", in *ACM Int. Worksh. Wirel. Mob. Multimed. WoWMoM*, Seattle, USA, 1999, pp. 26–33.

[3] B. Bellur, R. G. Ogier, and F. L. Templin, "Topology broadcast based on reverse-path forwarding routing protocol (tbrpf)", Internet Draft, 2003, draft-ietf-manet-tbrpf-06.txt

[4] T.-W. Chen and M. Gerla, "Global state routing: a new routing scheme for ad hoc wireless networks", in *Proc. IEEE ICC*, Atlanta, USA, 1998.

[5] S. Das, C. Perkins, and E. Royer, "Ad hoc on demand distance vector (AODV) routing", Internet Draft, 2002, draft-ietf-manet-aodv-11.txt

[6] H. Hassanein and A. Zhou, "Routing with load balancing in wireless ad hoc networks", in *Proc. ACM MSWiM*, Rome, Italy, 2001.

[7] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks", in *Proc. IEEE INMIC*, Orlando, USA, 2001.

[8] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", in *Proc. Fourth Ann. ACM/IEEE Int. Conf. Mob. Comput. Netw. Mobicom'98*, Dallas, USA, 1998.

[9] UCLA Parallel Computing Laboratory and Wireless Adaptive Mobility Laboratory, "Glomosim scalable simulation environment for wireless and wired network systems", 2003, http://pcl.cs.ucla.edu/projects/glomosim/

[10] S. J. Lee and M. Gerla, "Dynamic load-aware routing in ad hoc networks", in *Proc. ICC 2001*, Helsinki, Finland, 2001.

[11] S. J. Lee and M. Gerla, "SMR: split multipath routing with maximally disjoint paths in ad hoc networks", in *Proc. ICC 2001*, Helsinki, Finland, 2001.

[12] Lucent, "Orinoco PC card", 2003, http://www.lucent.com/orinoco

[13] C. E. Perkins and T. J. Watson, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers", in *ACM SIGCOMM'94 Conf. Commun. Archit.*, London, UK, 1994.

[14] J. H. Song, V. Wong, and V. Leung, "Load-aware on-demand routing (laor) protocol for mobile ad hoc networks", in *IEEE Veh. Technol. Conf. VTC-Spring*, Jeju, Korea, 2003, pp. 1753–1757.

[15] K. Wu and J. Harms, "Load-sensative routing for mobile ad hoc networks", in *Proc. IEEE ICCCN'01*, Scottsdale, USA, 2001.

Mehran Abolhasan received the B.E. in computer engineering with honours from the University of Wollongong in 1999. He completed his Ph.D. in the School of Computer, Electrical and Telecommunications Engineering, University Wollongong in 2003. In July 2003, he started working as a Research Fellow with Smart Internet Technology CRC and Office of Information and Communication Technology (OICT) within the Department of Commerce in NSW. In July 2004, he joined the desert knowledge CRC and Telecommunication and IT Research Institute. His research interests are wireless and ad hoc network scalability, medium access control (MAC), unicast and multicast routing protocols and QoS. Doctor Abolhasan has authored several research publications in this area, and is currently a Member of IEEE.
e-mail: mehran@titr.uow.edu.au
Telecommunications and IT Research Institute (TITR)
University of Wollongong
Northfields Ave
Wollongong, NSW 2522, Australia

Justin Lipman received a B.E. in computer engineering and Ph.D. in telecommunications engineering from the University of Wollongong in 1999 and 2004, respectively. In 2003 he was employed as a Research Fellow with the Smart Internet Technology Cooperative Research Centre (CRC-SIT) working on the Nimity Project. In 2004, he moved to Alcatel Shanghai Bell's Research and Innovation Centre in Shanghai, China, as a project manager to lead an innovating team looking at future wireless communications. Doctor Lipman's research interests are diverse but focus in general upon mesh/ad hoc networks, 3G/B3G/4G networks, sensor networks and distributed systems.
e-mail: justin@titr.uow.edu.au
Telecommunications and IT Research Institute (TITR)
University of Wollongong
Northfields Ave
Wollongong, NSW 2522, Australia

Tadeusz A. Wysocki – for biography, see this issue, p. 23.

Paper

Effect of unequal power allocation in turbo coded multi-route multi-hop networks

Tadahiro Wada, Abbas Jamalipour, Kouji Ohuchi, Hiraku Okada, and Masato Saito

Abstract— Multi-hop ad hoc networks are promising candidates for next generation mobile communications. They have sufficient channel capacity to achieve high data rate transmission for large number of users. One advantage of multi-hop networks is to realize multi-route transmissions. Since information bit streams can be transmitted over multiple routes, we can obtain route diversity effect. In order to enhance the route diversity effect, we usually introduce forward error correction schemes. Turbo coding is one of suitable coding methods for multi-hop networks. The turbo encoder generates one message stream and two parity streams whilst the message stream is more important than the parity streams for achieving reliable communications. Thus an unequal power allocation to the message and parity streams could be effective in improving the performance. In this paper, the effect of unequal power allocation for turbo coded multi-hop networks is investigated. Assuming the channel as additive white Gaussian and binary symmetric, we will show considerable performance improvement by unequal power allocation in terms of the bit error rate performance in multi-route multi-hop networks.

Keywords— multi-route transmissions, turbo codes, power allocation.

1. Introduction

For next generation mobile communications, the high channel capacity is required to realize high data rate transmission for large number of users. One way to achieve high channel capacity is to use small cell size such as pico cells. However, there is always the difficulty of installing large number of wired base stations for a small cell environment. One useful way to enhance the channel capacity without any substantial infrastructure increase is to realize a multi-hop ad hoc network [1–3]. By using a multi-hop network (because the transmitted data is relayed by mobile terminals) the data would virtually transmit in a small cell environment. A multi-hop network also has other essential advantages, such as good routing capability, small power consumption, guarantee of quality of communication service in poor channel conditions.

However, still there are some problems which prevent us to achieve a reliable and efficient use of the multi-hop networks. A major problem of the networks is to establish routes from a given source node to a given destination node. Since the topology of the network always changes by the movement of the source and intermediate nodes, routing of multi-hop network is a non-trivial work. Furthermore, battery operated mobile terminals require severe energy limitation for routing. Thus, many routing algorithms for the multi-hop networks have been studied. The most popular routing approach is on-demand routing [2, 3]. Instead of periodically exchanging route information in order to maintain routing table, on-demand routing protocols establish routes only when a source node requires data transmission. Since the protocols need to flood the pilot packets over the network in order to discover the available routes (which may causes the small throughput degradation), they have the capability to built suitable routes against the frequent change of the topology.

By transmitting information on a multi-hop network, we can choose either a multi-route or a single-route transmission from the source node to the destination node. Figure 1 shows the concept of a two-route multi-hop network. The multi-route transmission has sufficient capability to achieve a reliable communication without a rapid and strict routing update. By every route helping one another, a diversity effect from the multi-route transmissions can be obtained.

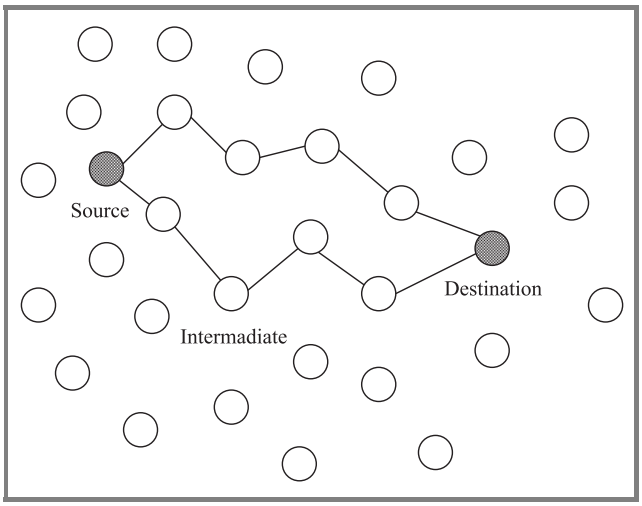


Fig. 1. Concept of route diversity in multi-hop networks.

One problem is how to use multi routes for reliable communications. There are two options in considering how to use the alternative route in multi-route transmission. The first one is that the alternative route can be used when the primary route is broken [2] and the second option is that an alterative route is simultaneously used for the transmission with the primary route [3]. Although the latter approach increases the number of packets (which may de-

grade throughput performance), it has enough capability to achieve reliable communications under the severe wireless environment by a diversity effect, namely the "route diversity."

In order to enhance the diversity effect, forward error correction (FEC) schemes should be introduced. By transmitting the same information for all routes, the effect of a repetition coding can be obtained. Since the repetition coding is trivial, another coding method which gives better performance should be considered. In this paper, turbo coding is adopted as the suitable FEC scheme for a multi-route transmission.

Turbo codes, proposed by Berrou *et al.* in 1993 [4], are very attractive means to improve the bit error rate (BER) performance. They are capable of operating at near Shannon capacity in an additive white Gaussian noise (AWGN) channel. Turbo encoder generates one message stream and two parity streams. The message stream essentially contains important information compared with parity streams. Thus it can be expected that reliability of communications increases if the message stream is transmitted on the route having good channel condition. Furthermore, we also expect to obtain a performance improvement by a suitable power allocation to the streams for a multi-route transmission.

In this paper, the effect of the route diversity in multi-route multi-hop networks using turbo codes is examined. In order to enhance the effect of the turbo codes, we investigate the suitable power allocation of turbo codes for multi-route networks assuming that every route has the same channel condition. First, we provide a brief introduction of turbo coding and explain the effect of unequal power allocation to message and parity streams. Next the effectiveness of unequal power allocation is examined. The BER performances with the AWGN channel and the binary symmetric channel (BSC) are introduced before concluding the paper.

2. Turbo codes and route diversity

2.1. Overview of turbo codes and route diversity

A typical structure of turbo encoder is illustrated in Fig. 2. The turbo encoder consists of two recursive systematic convolutional (RSC) element encoders, an interleaver and a puncturing algorithm. Each element encoder generates one message stream and one parity stream. Because the turbo encoder has two RSC element encoders, it generates two message streams, $\mathbf{x}^m$ and $\mathbf{x}^{m_2}$, and two parity streams, $\mathbf{x}^{p_1}$ and $\mathbf{x}^{p_2}$. Since two message streams have the same information, we usually transmit only $\mathbf{x}^m$ in order to improve the coding rate. This fact indicates that the message stream essentially contains very important information compared with the parity streams [5]. For high reliable communications in severe channel condition such as in a low signal-to-noise ratio (SNR) channel, we should consider a way to protect the message stream from disturbances, e.g., a large noise and severe fading.

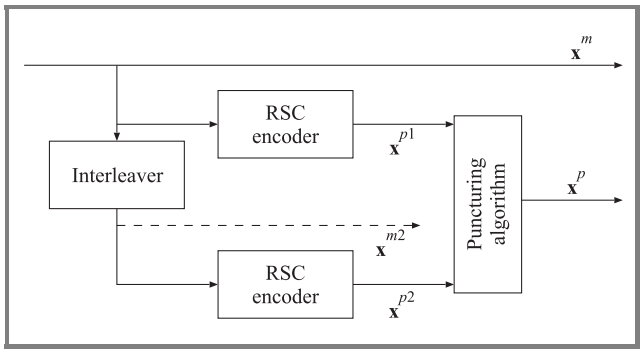


Fig. 2. Block diagram of turbo encoder with coding rate $1/2$.

An effective way for this protection is unequal power allocation to the message and parity streams [5]. By allocating larger power to the message stream compared with the parity streams, we can achieve reliable communication in a low SNR channel[1]. Let $\lambda(=\lambda_m/\lambda_p)$ be the power allocation ratio, where λ_m and λ_p correspond to the power allocated to the message and parity streams, respectively. In the case of rate $1/2$ turbo codes, we assume $\lambda_m+\lambda_p=1$. The message and parity signals should be amplified by $\sqrt{\lambda/(1+\lambda)}$ and $\sqrt{1/(1+\lambda)}$. On the other hand, in the case of rate $1/3$ turbo codes, we can assume $\lambda_m+2\lambda_p=1$ by allocating the same power to both parity streams, $\mathbf{x}^{p_1}$ and $\mathbf{x}^{p_2}$, respectively. In this case, the amplification factor for the message signal and for the parity signals are $\sqrt{\lambda/(2+\lambda)}$ and $\sqrt{1/(2+\lambda)}$, respectively.

2.2. Brief review of iterative decoding

We introduce the Bahl-Cocke-Jelinek-Raviv (BCJR) algorithm for iterative decoding for turbo codes [8]. Figure 3 shows a block diagram of iterative decoder, where $\mathbf{y}^m$, $\mathbf{y}^{p_1}$ and $\mathbf{y}^{p_2}$ are received streams for $\mathbf{x}^m$, $\mathbf{x}^{p_1}$, and $\mathbf{x}^{p_2}$, respectively. The decoder has two element decoders operated by a maximum a posteriori (MAP) probability decoding algorithm. L^{ej} denotes extrinsic information from jth MAP decoder.

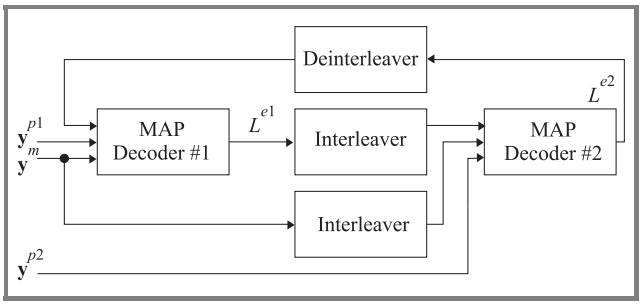


Fig. 3. Block diagram of iterative decoder.

[1]It should be noted that it is difficult to obtain a desirable performance by allocating large power to the message stream at high SNR. The performance of rate 1/3 turbo codes usually has an improvement by allocating large power to the parity stream in the case of a good channel condition, e.g., on near an error floor region [6, 7].

As it is known, the logarithm of a posteriori probability (LAPP) for kth bit, $L(u_k)$, is given by [8]

$$\begin{aligned} L(u_k) &= \lg\left(\frac{P(u_k=+1|\mathbf{y})}{P(u_k=-1|\mathbf{y})}\right) \\ &= \lg\left(\frac{\sum\limits_{S^+}(s_{k-1}=s',s_k=s,\mathbf{y})/p(\mathbf{y})}{\sum\limits_{S^-}(s_{k-1}=s',s_k=s,\mathbf{y})/p(\mathbf{y})}\right) \\ &= \lg\left(\frac{\sum\limits_{S^+}\alpha_{k-1}(s')\gamma_k(s',s)\beta_k(s)}{\sum\limits_{S^-}\alpha_{k-1}(s')\gamma_k(s',s)\beta_k(s)}\right), \end{aligned} \tag{1}$$

where $\gamma_k(s',s)$ is defined as

$$\gamma_k(s',s) = p(s_k=s,y_k|s_{k-1}=s'). \tag{2}$$

$\mathbf{y}$ is the received signal, $s_k \in S$ is the state of the encoder at time k, S^+ is the set of ordered pairs (s',s) corresponding to all state transitions $(s_{k-1}=s') \to (s_k=s)$ caused by data input $u_k=+1$, and S^- is similarly defined for $u_k=-1$.

$\alpha_k(s)$ and $\beta_k(s')$ are derived by recursive calculation as shown in the following:

$$\alpha_k(s) = \sum_{s'\in S}\alpha_{k-1}(s')\gamma_k(s',s), \tag{3}$$

$$\beta_{k-1}(s') = \sum_{s\in S}\beta_k(s)\gamma_k(s',s), \tag{4}$$

where the initial conditions for $\alpha_k(s)$ are $\alpha_0(0)=1$ and $\alpha_0(s\neq 0)=0$ and those for $\beta_k(s')$ are $\beta_N(0)=1$ and $\beta_N(s\neq 0)=0$.

The LAPP ratio can be expressed using Bayes' rule [9]:

$$L(u_k) = \lg\left(\frac{P(\mathbf{y}|u_k=+1)}{P(\mathbf{y}|u_k=-1)}\right) + \lg\left(\frac{P(u_k=+1)}{P(u_k=-1)}\right). \tag{5}$$

The second term is a priori information and is denoted as L_k^e, i.e.,

$$L_k^e = \lg\left(\frac{P(u_k=+1)}{P(u_k=-1)}\right). \tag{6}$$

The L_k^e is provided by the previous decoder on the iterative decoding.

By using L_k^e, the value of $\gamma_k(s',s)$ is given by

$$\gamma_k(s',s) \propto \exp\left(\frac{1}{2}u_k(L_k^e + L_c^m y_k^m) + \frac{1}{2}L_c^p y_k^p x_k^p\right), \tag{7}$$

where y_k^m is the kth received signal corresponding to the message bit x_k^m and y_k^p is one corresponding to the parity bit x_k^p.

L_c^m and L_c^p are channel information of the message and parity streams, respectively. In an AWGN channel, they are expressed as

$$\begin{aligned} L_c^m &= 2r\lambda_m E_b/(N_0/2) \\ L_c^p &= 2r\lambda_p E_b/(N_0/2), \end{aligned} \tag{8}$$

where r is the code rate of turbo coding. In the case of the equal power allocation, we obviously obtain $L_c^m = L_c^p$.

2.3. Binary symmetric channels assumption of multi-hop networks

In multi-hop networks, multiple routes can be assumed to be binary symmetric channels [10]. When the bit streams are relayed by intermediate nodes, we have to face a severe power restriction. In order to reduce the load in these nodes, we employ a hard decision for all bits in the stream and reconstruct the new stream which is passed to the next node. This procedure can significantly reduce the energy consumption.

In usual, the SNR at the receiver is measured and the result of the measurement is utilized as the channel information. But in multi-hop networks, the SNR estimation at the received side is of no worth for the iterative decoder because every received signal is multiple hopped and hard detected at the intermediate nodes. Therefore, the result of the SNR measurement does not reflect the whole route except for the final hop. One solution to obtain the channel information is that we assume the channel as a BSC and estimate the channel condition by counting errors of pilots at the destination node. In this paper, therefore, the effect of the unequal power allocation on the BSC is introduced as well.

In this paper, to enhance the effect of the unequal power allocation, the destination node is assumed to know the ideal BER performance. The channel information of the BSC are introduced in [11, 12]. In the BSC, the terms in Eq. (7), $L_c^m y_k^m$ and $L_c^p y_k^p$ should be replaced to $R^m Y_k^m$ and $R^p Y_k^p$, respectively, where $Y_k^m = \lambda_m \mathrm{sgn}(y_k^m)$ and $Y_k^p = \lambda_p \mathrm{sgn}(y_k^p)$. Terms R_m and R_p indicate the channel information for the BSC and are derived as follows:

$$\begin{aligned} R^m &= \ln\frac{1-P_m}{P_m}, \\ R^p &= \ln\frac{1-P_p}{P_p}, \end{aligned} \tag{9}$$

where P_m and P_p are BER performance of the message and the parity streams, respectively. If every link is affected by AWGN, P_m and P_p can be expressed as follows:

$$\begin{aligned} P_m &\simeq MQ(2r\lambda_m E_b/N_0), \\ P_p &\simeq MQ(2r\lambda_p E_b/N_0), \end{aligned} \tag{10}$$

where M denotes the number of hops and $Q(t) = (1/\sqrt{2\pi})\int_t^\infty \exp(-\tau^2/2)d\tau$.

3. Numerical results

3.1. System model and assumptions for simulations

Some numerical examples are shown in this section. In order to obtain essential performances of turbo codes on route diversity, we make ideal assumptions to simplify the evaluation.

First, the number of routes from the source node to the destination node is assumed to be two or three and the routes

are statistically independent. This assumption is actually appropriate because we may have difficulty in finding large number of statistical independent routes. We consider that each message and parity stream transmits on its own route. In the AWGN channel, the variance of the noise is assumed to be the same for all routes and the destination node knows the ideal SNR value. In the BSC, we assume the destination node knows the BER performance of all routes.

Figure 4 illustrates the system model of rate $1/3$ turbo encoder with unequal power allocation. It has two (31,27) RSC element encoders and a random interleaver with the length of 5000.

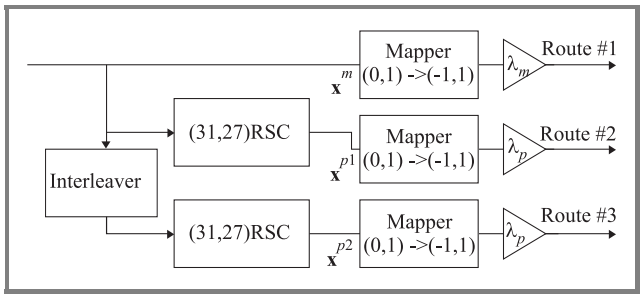


Fig. 4. System model of turbo encoder for performance evaluation. The code rate of this system is 1/3.

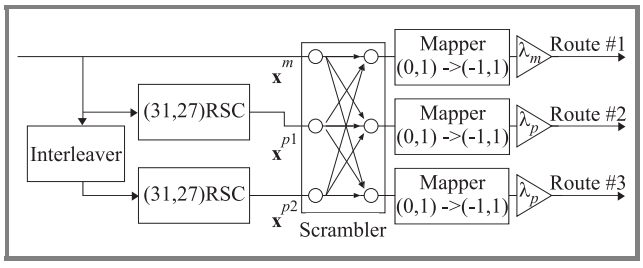


Fig. 5. System model of turbo encoder having a scrambler. The code rate of this system is 1/3.

In order to emphasize the effectiveness of unequal power allocation, we derive another performance, which comes from Fig. 5. This figure shows the system model of turbo encoder having a scrambler which scrambles the message and parity streams. Since we can make the importance of all streams be equal by scrambling the streams, it can be expected to neglect the effect of unequal power allocation. The permutation rule of the scrambler for the rate $1/3$ encoder is assumed as following:

$$\begin{aligned}\mathbf{x}^1 &= (\cdots, x_k^m, x_{k+1}^{p_2}, x_{k+2}^{p_1}, \cdots),\\ \mathbf{x}^2 &= (\cdots, x_k^{p_1}, x_{k+1}^m, x_{k+2}^{p_2}, \cdots),\\ \mathbf{x}^3 &= (\cdots, x_k^{p_2}, x_{k+1}^{p_1}, x_{k+2}^m, \cdots),\end{aligned} \tag{11}$$

where $\mathbf{x}^i$ is the scrambled stream transmitting on the ith route, $i = 1, 2, 3$. Of course a descrambler at the receiving end is required. Assuming that we allocate the same power, expressed as λ_2, to $\mathbf{x}^2$ and $\mathbf{x}^3$ and another power allocated to $\mathbf{x}^1$, expressed as λ_1. The ratio of the allocated powers, λ_1/λ_2, is expressed as λ.

Although Figs. 4 and 5 illustrate rate $1/3$ turbo encoders, the performances of not only rate $1/3$ but rate $1/2$ turbo codes can be derived. The permutation rule of the scrambler for the rate $1/2$ encoder is

$$\begin{aligned}\mathbf{x}^1 &= (\cdots, x_k^m, x_{k+1}^m, x_{k+2}^{p_1}, x_{k+3}^{p_2} \cdots)\\ \mathbf{x}^2 &= (\cdots, x_k^{p_1}, x_{k+1}^{p_2}, x_{k+2}^m, x_{k+3}^m \cdots).\end{aligned} \tag{12}$$

The iteration number for the decoding process is set to 10.

3.2. Effect of unequal power allocation in AWGN channel

Figures 6 and 7 show the BER performance with the unequal power allocation for rates $1/2$ and $1/3$ turbo codes, respectively. We set the range of the power allocation ratio, λ, between 0.8 and 2.0, where $\lambda = 1$ is a typical value.

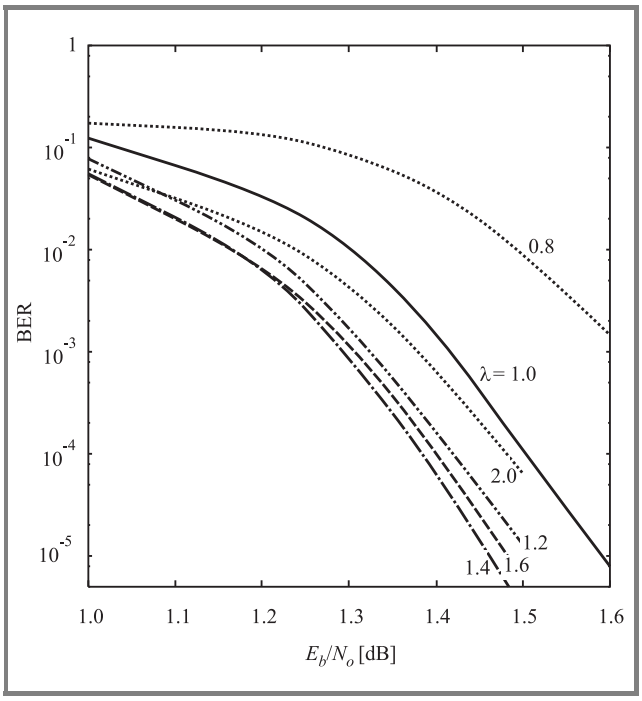


Fig. 6. Bit error rate performance versus E_b/N_0 for varying the power allocation ratio. The code rate is set at $1/2$.

From the results, we find the effectiveness of the unequal power allocation. When the power allocated to the message streams decreases, i.e., $\lambda = 0.8$, the BER performance degrades in both coding rates. In contrast, we observe performance improvement by allocating a large power to the message stream. It can be found that a suitable unequal power allocation offers approximately a 0.15 dB performance improvement over the equal power allocation.

Figures 8 and 9 show the BER performance with a scrambler for rates $1/2$ and $1/3$ turbo codes, respectively. The range of the power allocation ratio is from 0.8 to 2.0. From these figures, it can be found that the BER performance at $\lambda = 1$ is the best, i.e, we face the performance degradation with scrambling the streams by unequal power allocation.

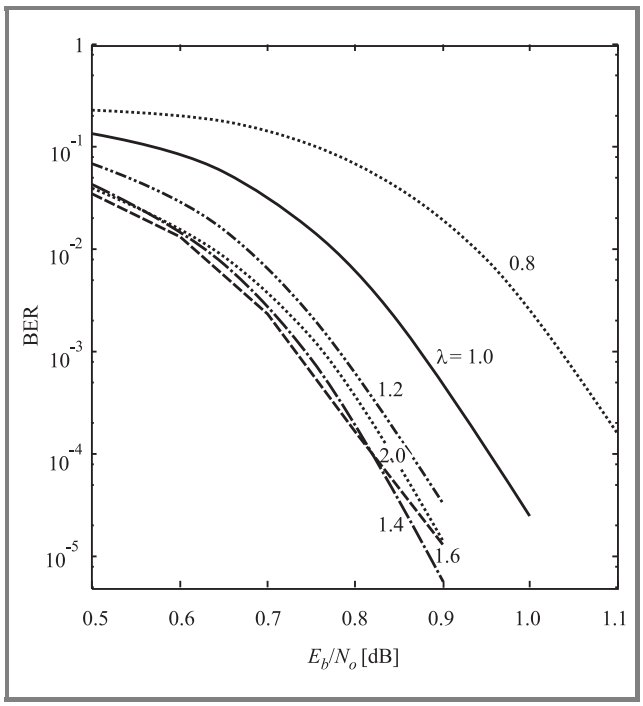


Fig. 7. BER performance versus E_b/N_0 for varying the power allocation ratio. The code rate is set at $1/3$.

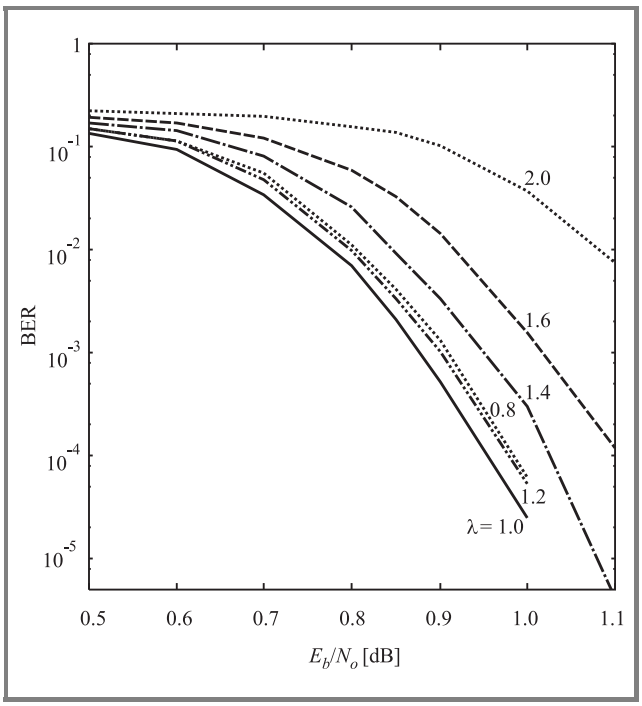


Fig. 9. BER performance versus E_b/N_0 for varying the power allocation ratio with the scrambler. The code rate is set at $1/3$.

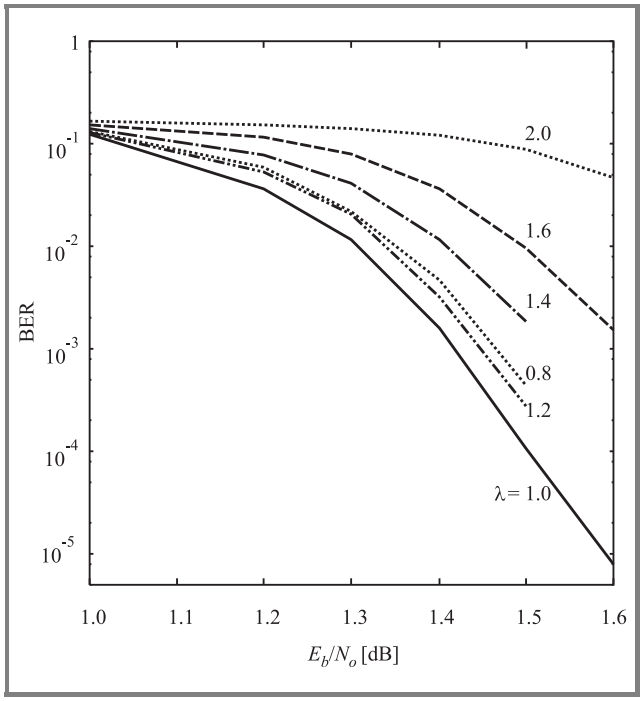


Fig. 8. BER performance versus E_b/N_0 for varying the power allocation ratio with the scrambler. The code rate is set at $1/2$.

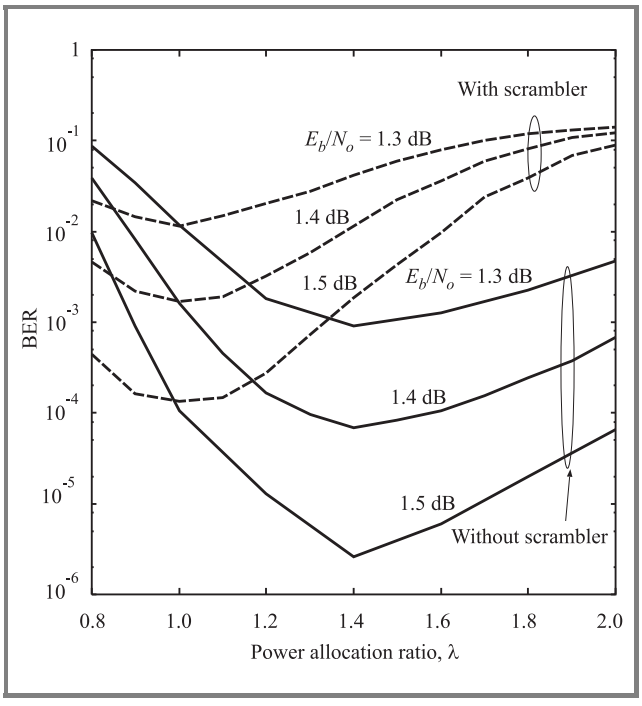


Fig. 10. BER performance versus λ. The code rate is $1/2$. The performances of both with and without the scrambler are plotted.

The results show that the importance of the message stream is neglected by the scrambling and we cannot obtain any performance improvement from unequal power allocation.

Figures 10 and 11 show the BER performance as a function of the power allocation ratio, λ, for rates $1/2$ and $1/3$ turbo codes, respectively. From Fig. 10, which indicates the performance of the rate $1/2$ codes, we can obtain the best performance by the unequal power allocation when λ is around 1.4. On the other hand, we can obtain the best performance when λ is around 1.5 in the case of rate $1/2$ turbo codes. We also find that the performance improvement can be kept over the wide range of λ.

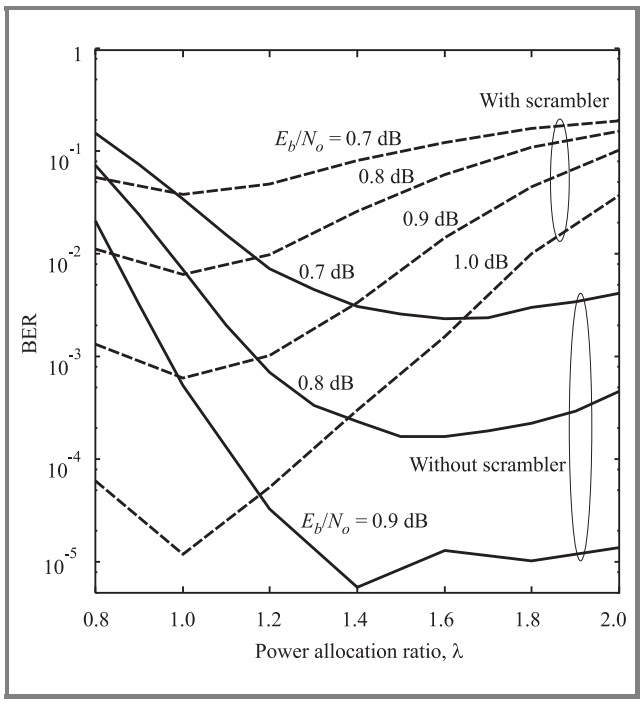


Fig. 11. Bit error rate performance versus the power allocation ratio when the code rate is $1/3$. The performances of both with and without the scrambler are plotted.

3.3. Effect of unequal power allocation in BSC

Figures 12 and 13 show BER performance with the unequal power allocation in the BSC. We do not utilize the scrambler in this subsection. We set the power allocation ratio, λ, between 0.8 and 2.0. As we expected, the BER performance with the BSC degrades compared with that of the AWGN channel. But the tendency of the performance of BSC is similar to that of the AWGN channel by changing the power allocation ratio, i.e., we can find performance improvement by allocating the large power to the message stream.

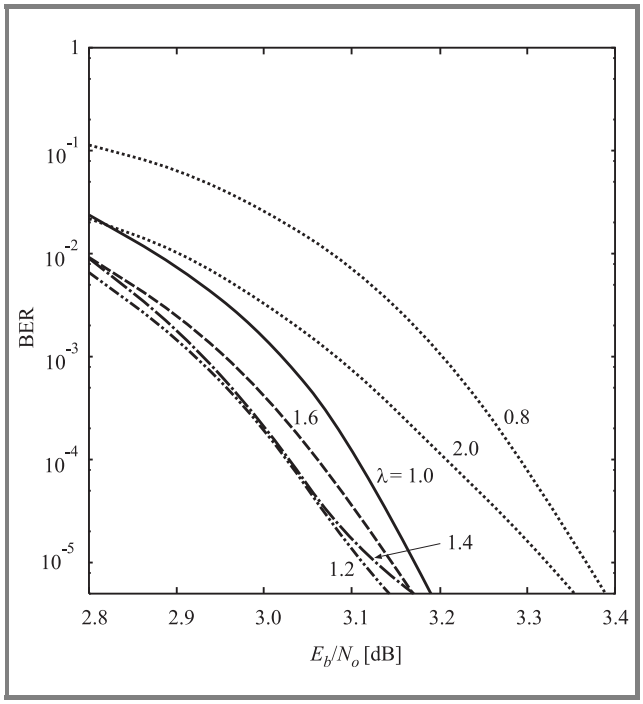


Fig. 12. Bit error rate performance versus E_b/N_0 for varying the power allocation ratio in the BSC. The code rate is set at $1/2$.

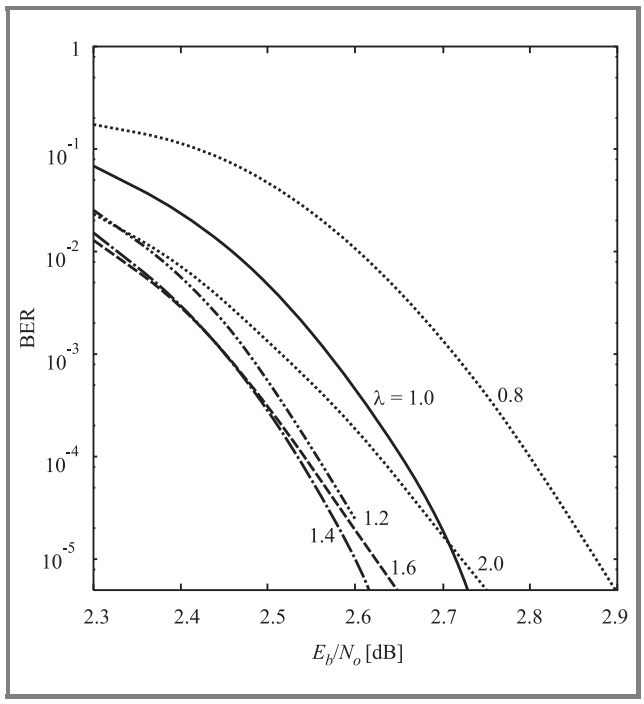


Fig. 13. Bit error rate performance versus E_b/N_0 for varying the power allocation ratio in the BSC. The code rate is set at $1/3$.

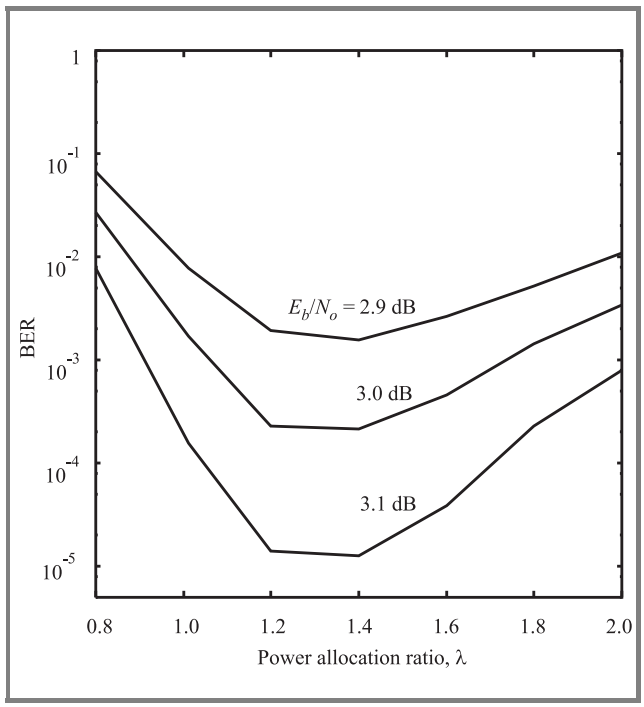


Fig. 14. Bit error rate performance versus the power allocation ratio when the code rate is $1/2$. The channel is assumed as the BSC.

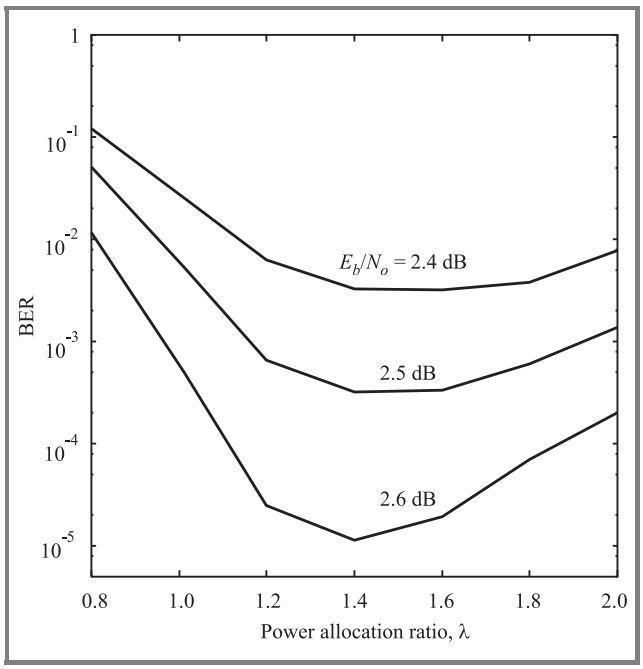


Fig. 15. Bit error rate performance versus the power allocation ratio when the code rate is $1/3$. The channel is assumed as the BSC.

Figures 14 and 15 illustrate the BER performance as a function of the power allocation ratio, λ, for rates $1/2$ and $1/3$ turbo codes, respectively. From Fig. 10, we can obtain the best performance when λ is around 1.3. On the other hand, we can obtain the best performance when λ is around 1.5 in the case of rate $1/2$ turbo codes. In contrast with the performance in Fig. 11, the performance improvement is not kept as λ increases.

4. Conclusions

In this paper, the effect of unequal power allocation to message and parity streams in turbo coded multi-route networks by route diversity was investigated. Additive white Gaussian and binary symmetric channels have been used. It is found that it is possible to obtain considerable performance improvement by allocating larger power to the message stream compared with that of the parity stream. The results suggest that unequal power allocation is an efficient way in improving the bit error rate performance in multi-hop networks. Although in this paper all routes have been assumed to have similar channel conditions, each route actually could have its own condition. The results also suggest that a suitable power allocation can prevent performance degradation by taking individual channel conditions into account.

Acknowledgements

This work is partially supported by Strategic Information and Communications R&D Promotion Programme (SCOPE) by Ministry of Internal Affairs and Communications, Japan.

References

[1] S. Toumpis and A. J. Goldsmith, "Capacity regions for wireless ad hoc networks", *IEEE Trans. Wirel. Commun.*, vol. 2, no. 4, pp. 736–748, 2003.

[2] A. Nasipuri and S. R. Das, "On-demand multipath routing for mobile ad hoc networks", in *IEEE Int. Conf. Comput. Commun. Netw.*, Boston, USA, 1999, pp. 64–70.

[3] S.-J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", in *IEEE Int. Conf. Commun.*, Helsinki, Finland, 2001, pp. 3201–3205.

[4] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding: turbo-codes", in *Int. Conf. Commun.*, Geneva, Switzerland, 1993, pp. 1064–1070.

[5] J. Hokfelt and T. Maseng, "Optimizing the energy of different bit-streams of turbo codes", in *Turbo Cod. Sem. Proc.*, Lund, Sweden, 1996, pp. 59–63.

[6] T. M. Duman and M. Salehi, "On optimal power allocation for turbo codes", in *Int. Symp. Inform. Theory*, Ulm, Germany, 1997, p. 104.

[7] S.-J. Park and S. W. Kim, "Transmission power allocation in turbo codes", in *Veh. Technol. Conf. 2000*, Boston, USA, 2000, pp. 2073–2075.

[8] W. E. Ryan, "A turbo code tutorial", www.ece.arizona.edu/∼ryan/

[9] D. Applebaum, *Probability and Information*. Cambridge: Cambridge University Press, 1996.

[10] T. Wada, N. Nakagawa, H. Okada, A. Jamalipour, K. Ohuchi, and M. Saito, "Performance improvement of turbo coded multi-route multi-hop networks using parity check codes", in *2005 IEEE Worksh. High Perform. Switch. Rout.*, Hong Kong, China, 2005.

[11] 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, 1996.

[12] C. Zheng, T. Yamazato, H. Okada, M. Katayama, and A. Ogawa, "A study on turbo soft-decision decoding for hard-detected optical communication signals", *IEICE Trans. Commun.*, vol. 86, no. 3, pp. 1022–1030, 2003.

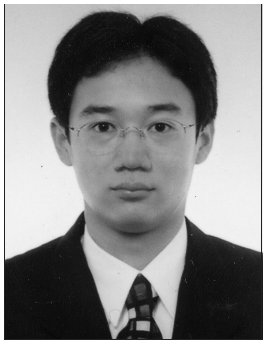
Tadahiro Wada was born in Gifu, Japan, in 1969. He received the B.E. degree in electrical, electronic and information engineering from Nagoya University in 1993, and the M.E. and Ph.D. degrees in information electronics from Nagoya University in 1995 and 1997, respectively. Since April 1998, he was with Department of Electrical and Electronics Engineering in Shizuoka University, Japan, as an Assistant Professor. From 2004 to 2005, he was a Visiting Scholar at the School of Electrical and Information Engineering, University of Sydney, Australia. Since 2005, he has been a lecturer in Division of Applied Science and Basic Engineering, Shizuoka University, Japan. His research interests lie in the areas of spread-spectrum communications, satellite communications, CDMA systems, power line communications, coding theory and mobile communications. He was a recipient of the IEICE Young Investigators Award in 2002. Doctor Wada is a Member of IEEE, IEICE, and SITA.
e-mail: tetwada@ipc.shizuoka.ac.jp
Department of Electrical and Electronic Engineering
Shizuoka University Johoku 3-5-1
Hamamatsu, 432-8561 Japan

Abbas Jamalipour received the Ph.D. degree in electrical engineering from Nagoya University, Nagoya, Japan. He is a Professor at the School of Electrical and Information Engineering, University of Sydney, Australia, where he is responsible for teaching and research in wireless data communication networks, wireless IP networks, network security, and satellite systems. He is the author for the first technical book on networking aspects of wireless IP, "The Wireless Mobile Internet – Architectures, Protocols and Services" (Chichester: Wiley, 2003). In addition, he has authored another book on satellite communication networks, "Low Earth Orbital Satellites for Personal Communication Networks" (Norwood: Artech House, 1998) and coauthored four other technical books in wireless telecommunications. He has authored over 150 papers in major journals and international conferences, and given short courses and tutorials in major international conferences. He is the Editor-in-Chief of the "IEEE Wireless Communications" and a Technical Editor of the "IEEE Communications", and the "International Journal of Communication Systems". Professor Jamalipour is the Technical Program Vice-Chair of IEEE WCNC 2005, Co-Chair of Symposium on Next Generation Networks, IEEE ICC 2005, Technical Program Vice-Chair IEEE HPSR 2005, Chair of the Wireless Communications Symposium, IEEE GLOBECOM 2005, and Co-Chair of Symposium on Next Generation Mobile Networks, IEEE ICC 2006. He is a Fellow Member of IEAust; Chair of IEEE Communications Society Satellite and Space Communications Technical Committee; Vice Chair of Asia Pacific Board, Technical Affairs Committee; and Vice Chair of Communications Switching and Routing Technical Committee. He is a Distinguished Lecturer of the IEEE Communications Society and a Senior Member of IEEE.

e-mail: a.jamalipour@ieee.org
School of Electrical and Information Engineering
The University of Sydney
Sydney, NSW 2006, Australia

Kouji Ohuchi was born in Ibaraki, Japan, in 1970. He received the B.E., M.E. and E.D. degrees from Ibaraki University, Japan, in 1994, 1996, and 1999, respectively. He has been a Research Associate at Graduate School of Electronic Science and Technology, Shizuoka University, since 1999. He is a Member of IEEE and IEICE. His research interests are in spread spectrum communications, synchronization systems, and error correcting techniques.

e-mail: dkoouti@ipc.shizuoka.ac.jp
Graduate School of Electronic Science
and Engineering
Shizuoka University Johoku 3-5-1
Hamamatsu, 432-8561 Japan



Hiraku Okada received the B.Sc., M.Sc. and Ph.D. degrees in information electronics engineering from Nagoya University, Japan, in 1995, 1997 and 1999, respectively. From 1997 to 2000, he was a Research Fellow of the Japan Society for the Promotion of Science. Since 2000, he has been an Assistant Professor of the Center for Information Media Studies at Nagoya University, Japan. His current research interests include the packet radio communications, multimedia traffic, wireless multi-hop/multi-cell networks, and CDMA technologies. He received the Inose Science Award in 1996, and the IEICE Young Engineer Award in 1998. Doctor Okada is a Member of IEEE, IEICE, and SITA.

e-mail: okada@nuee.nagoya-u.ac.jp
EcoTopia Science Institute
Nagoya University
Furo-cho, Nagoya, 464-8603 Japan

Masato Saito received the B.E., M.E., and Ph.D. degrees from Nagoya University, Japan, in 1996, 1998, 2001, respectively. He is currently an Assistant Professor of the Graduate School of Information Science at Nara Institute of Science and Technology (NAIST), Japan. His current research interests include spread-spectrum modulation schemes, mobile communications, CDMA schemes, multi-carrier modulation schemes, packet radio networks, and multi-hop networks. Doctor Saito is a Member of IEEE and IEICE.

e-mail: saito@is.aist-nara.ac.jp
Graduate School of Information Science
Nara Institute of Science and Technology (NAIST)
8916-5 Takayama-cho
Ikoma, Nara, 630-0192 Japan

Paper

An adaptive iterative receiver for space-time coding MIMO systems

Chakree Teekapakvisit, Van Dong Pham, and Branka Vucetic

Abstract—An adaptive iterative receiver for layered space-time coded (LSTC) systems is proposed. The proposed receiver, based on a joint adaptive iterative detection and decoding algorithm, adaptively suppresses and cancels co-channel interference. The LMS algorithm and maximum a posteriori (MAP) algorithm are utilized in the receiver structure. A partially filtered gradient LMS (PFGLMS) algorithm is also applied to improve the convergence speed and tracking ability of the adaptive detector with a slight increase in complexity. The proposed receiver is analysed in a slow and fast Rayleigh fading channels in multiple input multiple output (MIMO) systems.

Keywords— adaptive equalizer, iterative detection, layered space-time coding, LMS, PFGLMS.

1. Introduction

Multiple input multiple output (MIMO) systems have recently emerged as one of the most significant technical advances in modern communications. This technology promises to solve the capacity bottleneck in wireless communication systems [1]. It was shown in [2] that a Diagonal Bell Laboratories Layered Space-Time (DBLAST) MIMO system using a combination of forward error control (FEC) codes can exploit spatial diversity to asymptotically achieve outage capacity. El Gamal *et al.* [3] proposed a threaded layered space-time code (TLSTC) structure, which has an improved bandwidth efficiency compared to the DBLAST structure.

In layered space-time coded (LSTC) systems, co-channel interference from adjacent layers limits the system performance. To reduce co-channel interference, two iterative receivers with combined detection and decoding are proposed in [3] and [4], based on the turbo principle. The first scheme implements minimum mean square error (MMSE) detection with soft-output Viterbi algorithm (SOVA) decoding in the iterative receiver. The second approach proposes a combination of parallel interference cancellation (PIC) detection with maximum a posteriori (MAP) decoding. Both approaches depend on additional channel estimation, and exhibit near interference-free single user performance for certain ranges of the signal to noise ratio (SNR) under the assumption of perfect channel state information (CSI) at the receiver. Recently, an adaptive co-channel interference cancellation scheme for an STC system was proposed in [5]. However, the adaptive receiver design is based on linear detection, which could suffer a performance degradation in a high interference environment. Therefore, a non-linear adaptive detection is necessary for improving the performance of the receiver.

In this paper, a new adaptive iterative TLSTC receiver is proposed based on a joint adaptive iterative detection and decoding algorithm. The proposed receiver does not require channel state information as the non-adaptive iterative receivers in [3] and [4]. Therefore, the proposed receiver does not require a matrix inversion process in the system. As a result, the complexity of the proposed receiver is less than that of the non-adaptive iterative receiver. Moreover, this adaptive iterative receiver has the advantage of combining co-channel interference suppression and cancellation. In this paper, we are mainly concerned with the performance gain due to interference cancellation and tracking ability of the adaptive iterative structures. We show that the adaptive iterative receiver provides a significant performance improvement compared to a single iteration linear adaptive receiver.

The paper is organized as follow: Section 2 describes the LSTC systems and channel models as well as the proposed adaptive iterative receiver structure. The simulation results are discussed in Section 3, followed by the conclusion in Section 4.

2. System model

A threaded layered space-time coded transmitter structure for a single user is shown in Fig. 1. A structure consisting of N transmit and M receive antennas is considered throughout this paper. The binary information stream is converted by a serial to parallel converter and encoded by a convolutional encoder to produce a coded data stream for each layer, corresponding to each of the N transmit antennas. The layered coded data streams are then modulated and fed into a spatial interleaver to distribute a coded stream for all layers among N transmit antennas. After time interleaving, the coded symbols of each layer are simultaneously and synchronously transmitted from the N transmit

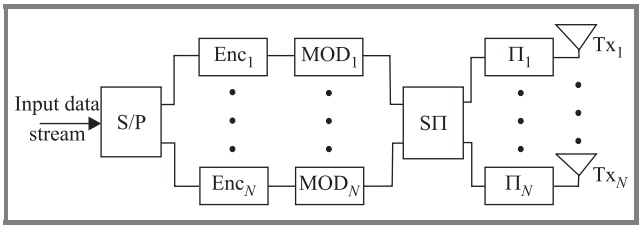


Fig. 1. Layered space-time transmitter structure.

antennas through the MIMO channel. The received signal at each of the M receive antennas can be considered as a superposition of all N transmitted symbols and additive white Gaussian noise (AWGN). The received signal vector, denoted by $\mathbf{r}$, can be represented as

$$\mathbf{r} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{r}$ is an $M \times 1$ column vector of the received signals across the M receive antennas, $\mathbf{H}$ is an $M \times N$ complex channel matrix gain, $\mathbf{x}$ is an $N \times 1$ vector of the transmitted symbols across the N transmit antennas and $\mathbf{n}$ is an $M \times 1$ vector of the AWGN noise with a zero mean and the noise variance of σ^2.

The iterative LSTC receiver structure is shown in Fig. 2. It consists of two stages: a soft-input soft-output (SISO) detector followed by N parallel SISO channel decoders. Time and spatial deinteleavers and spatial and time interleavers separate the two stages. The SISO detector employs an iterative MMSE interference canceller consisting of a feed-forward filter and a feedback filter.

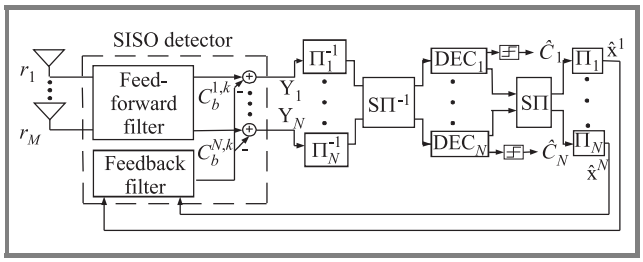


Fig. 2. Block diagram of iterative LST receiver.

In the first iteration, the feed-forward filter performs interference suppression without the interference cancellation process because there are no estimated symbols from the output of the MAP decoder. After the first iteration, the feedback filter is included into the detection process. The estimated symbols from the output of the decoder are fed back to the feedback filter to cancel the interference from other antennas in the detection process. The detected symbol obtained at the output of the MMSE detector in the kth iteration at time t, for layer i, denoted by $y_t^{i,k}$, is given by

$$y_t^{i,k} = \mathbf{w}_f^{i,k^T}\,\mathbf{r} + \mathbf{w}_b^{i,k^T}\,\underline{\hat{\mathbf{x}}}^{i,k}, \tag{2}$$

where $\mathbf{w}_j^{i,k}$ is an $M \times 1$ feed-forward coefficient vector, represented as $\mathbf{w}_f = \left[w_{f,0}, w_{f,1}, \ldots, w_{f,M-1}\right]^T$ and $\mathbf{w}_b^{i,k}$ is an $(N-1)\times 1$ feedback coefficient vector, that can be written in the form $\mathbf{w}_b = \left[w_{b,0}, w_{b,1}, w_{b,i-1}\, w_{b,j+1}, \ldots, w_{b,N-1}\right]^T$, and $\underline{\hat{\mathbf{x}}}^{i,k}$ is an $(N-1)\times 1$ vector of the estimated symbols from the output of the SISO MAP decoders at the kth iteration for other antennas, given as

$$\underline{\hat{\mathbf{x}}}^{i,k} = \left(\hat{x}_t^{1,k}, \hat{x}_i^{2,k}, \ldots, \hat{x}_t^{i-1,k}, \hat{x}_t^{i+1,k}, \ldots, \hat{x}_t^{N,k}\right). \tag{3}$$

The second term in Eq. (2) represents the cancelled interference, denoted by a scalar feedback coefficient $c_b^{i,k}$ and given by

$$c_b^{i,k} = \mathbf{w}_b^{i,k^T}\,\underline{\hat{\mathbf{x}}}^{i,k}. \tag{4}$$

The values of $\mathbf{w}_j^{i,k}$ and $c_b^{i,k}$ are calculated by minimizing the mean square error between the transmitted symbol and its estimate, given by

$$e = E\left[\left|y_t^{i,k} - x_t^{i,k}\right|^2\right]. \tag{5}$$

Let us assume that there is a perfect knowledge of the channel coefficients matrix $\mathbf{H}$. Define $\mathbf{H}_i$ as the ith column of the channel matrix $\mathbf{H}$, representing an $M \times 1$ vector of the complex channel gains for the ith transmit antenna, $\mathbf{H}_i^{\mathbf{H}}$ is a conjugate transpose of $\mathbf{H}_i$ and $\underline{\mathbf{H}}^i$ is an $M \times (N-1)$ matrix composed of the complex channel gains for the other $(N-1)$ transmit antennas. Also define

$$\mathbf{A} = \mathbf{H}_i\,\mathbf{H}_i^{\mathbf{H}}, \tag{6}$$

$$\mathbf{B} = \underline{\mathbf{H}}^i\left[\mathbf{I}_{N-1} - diag\left(\underline{\hat{\mathbf{x}}}^{i,k}\,\underline{\hat{\mathbf{x}}}^{i,k^T}\right) + \underline{\hat{\mathbf{x}}}^{i,k}\,\underline{\hat{\mathbf{x}}}^{i,k^T}\right]\underline{\mathbf{H}}^{i\mathbf{H}}, \tag{7}$$

$$\mathbf{D} = \underline{\mathbf{H}}^i\,\underline{\hat{\mathbf{x}}}^{i,k}, \tag{8}$$

$$\mathbf{R} = \sigma^2\mathbf{I}_M, \tag{9}$$

where $\mathbf{I}_{N-1}$ and $\mathbf{I}_M$ are $(N-1)\times(N-1)$ and $M \times M$ identity matrices, respectively. The optimum feed-forward and feedback coefficients are given by [6]

$$\mathbf{w}_j^{i,k^T} = \mathbf{H}_i^H\left(\mathbf{A} + \mathbf{B} + \mathbf{R} - \mathbf{D}\mathbf{D}^H\right)^{-1}, \tag{10}$$

$$c_b^{i,k^T} = -\mathbf{w}_j^{i,k^T}\,\mathbf{D}. \tag{11}$$

From Eq. (10), the complexity of computing an $M \times M$ inverse matrix is approximately in the order of M^3 [7]. Therefore, an adaptive algorithm is utilized in this paper to reduce a high computation complexity. The feed-forward coefficient vector $\mathbf{w}_j^{i,k}$ and feedback coefficient vector $\mathbf{w}_b^{i,k}$ defined in Eq. (2) are determined recursively by an adaptive least mean square (LMS) algorithm [8]. By using Eq. (2) to calculate the coefficients $\mathbf{w}_j^{i,k}(t)$ and $\mathbf{w}_b^{i,k}(t)$ adaptively for a particular time instant t, the mean squared error in Eq. (5) is given by

$$e(t) = E\left[\left|\mathbf{w}_j^{i,k^T}(t)\,\mathbf{r} + \mathbf{w}_b^{i,k^T}(t)\,\underline{\hat{\mathbf{x}}}^{i,k} - x_i^{i,k}\right|^2\right], \tag{12}$$

where

$$\mathbf{w}_j^{i,k}(t+1) = \mathbf{w}_j^{i,k}(t) + \mu_f e(t)\,\mathbf{r}(t), \tag{13}$$

$$\mathbf{w}_b^{i,k}(t+1) = \mathbf{w}_b^{i,k}(t) + \mu_b e(t)\,\underline{\hat{\mathbf{x}}}(t), \tag{14}$$

μ_f and μ_b are the step sizes for the feed-forward and feedback adaptations, respectively. As the LMS algorithm

has a slow convergence, the partially filtered gradient LMS (PFGLMS) [9] algorithm based on an exponentially weighted least square error is used to improve the convergence speed of the LMS algorithm with a slight increase in complexity.

The conventional LMS algorithm requires $2M+1$ multiplications and the same number of additions for each received data symbol. However, the PFGLMS algorithm requires $4M+1$ multiplications and the same number of additions for each received data symbol. Therefore, the computation complexity is approximately in the order of M for both LMS and PFGLMS algorithm.

The modified feed-forward and feedback coefficients of the PFGLMS algorithm for MIMO systems are given by

$$\mathbf{w}_j^{i,k}(t+1) = \mathbf{w}_j^{i,k}(t) + \mu_f e(t)\,\mathbf{g}_j^{i,k}(t), \tag{15}$$

$$\mathbf{w}_b^{i,k}(t+1) = \mathbf{w}_b^{i,k}(t) + \mu_b e(t)\,\mathbf{g}^{i,k}(t), \tag{16}$$

where

$$\left.\begin{aligned} \mathbf{g}_f^{i,k}(t) &= e(t)\,\mathbf{x}(t) + \hat{\mathbf{g}}_f^{i,k}(t) \\ \hat{\mathbf{g}}_f^{i,k}(t) &= \lambda_f \hat{\mathbf{g}}_f^{i,k}(t-1) + \gamma_f e(t)\,\mathbf{x}(t) \end{aligned}\right\}, \tag{17}$$

$$\left.\begin{aligned} \mathbf{g}_b^{i,k}(t) &= e(t)\,\mathbf{x}(t) + \hat{\mathbf{g}}_b^{i,k}(t) \\ \hat{\mathbf{g}}_b^{i,k}(t) &= \lambda_b \hat{\mathbf{g}}_b^{i,k}(t-1) + \gamma_b e(t)\,\mathbf{x}(t) \end{aligned}\right\}, \tag{18}$$

where (λ_f, λ_b) and (γ_f, γ_b) are the forgetting factors and the scaling factors, respectively, and $\hat{\mathbf{g}}_f^{i,k}(0) = \hat{\mathbf{g}}_b^{i,k}(0) = 0$. In the proposed receiver structure, the well-known SISO MAP decoder takes the detection output of the detector, $y_t^{i,k}$, as a soft-input to the decoder.

The soft-output from the decoder is used to calculate the interference, which is subtracted for the decoder input in the next iteration. This iterative detection/decoding process is performed until the symbol estimate converges to the optimal performance. The soft-output from the decoder in the last iteration is then fed into a decision device to produce a decision. A BPSK modulation scheme is used.

The likelihood functions for the transmitted modulated symbols 1 and -1 can be written as [10]

$$P\left(y_t^{i,k} \middle| x_t^{i,k} = \pm 1\right) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp \frac{-\left(y_t^{i,k} \mp 1\right)^2}{2\sigma^2}. \tag{19}$$

The log-likelihood ratios (LLR) determined in the kth iteration for the ith transmit layer, denoted by $\lambda_i^{i,k}$, are given by

$$\lambda_i^{i,k} = \log\left(\frac{P\left(x_t^{i,k}=1 \middle| y_t^{i,k}\right)}{P\left(x_t^{i,k}=-1 \middle| y_t^{i,k}\right)}\right). \tag{20}$$

The symbol a posteriori probabilities (APP) $P(x_t^{i,k} = q \big| y_t^{i,k}, q = 1, -1)$ conditioned on the output variable $y_t^{i,k}$ can then be obtained as

$$P\left(x_t^{i,k}=1 \middle| y_t^{i,k}\right) = \frac{e^{\lambda_t^{i,k}}}{e^{\lambda_t^{i,k}}+1}, \tag{21}$$

$$P\left(x_t^{i,k}=-1 \middle| y_t^{i,k}\right) = \frac{1}{e^{\lambda_t^{i,k}}+1}. \tag{22}$$

The soft-output symbols estimate in the ith layer and kth iteration can be determined as

$$x_t^{i,k} = \frac{e^{\lambda_t^{i,k}}-1}{e^{\lambda_t^{i,k}}+1}. \tag{23}$$

3. Performance results

This section presents simulation results for the LSTC non-adaptive and adaptive iterative receivers with BPSK modulation in slow and fast Rayleigh fading channels. The slow fading channel is modelled as a quasi-static fading channel, where each fading coefficient is constant within a frame, but changes from one frame to another and for each sub-channel. The system operates in the training mode until the mean square error (MSE) approaches the minimum mean square error, then it switches to the decision directed mode. The constituent codes are nonsystematic convolutional codes with the code rate R of 1/2, memory order of 3, and the generating polynomial $g_1 = 15_8$ and $g_2 = 17_8$. The proposed system is simulated with 2 transmit and 2 receive antennas, i.e., a 2×2 MIMO system, with 260 information bits in each frame. After serial to parallel conversion, each layer of the LSTC system consists of 130 information bits, followed by 266 encoded symbols per layer. The data rate is 1 Mb/s at the carrier frequency, f_c, of 2 GHz. The simulation results are represented in terms of the average bit error rate (BER) versus the ratio of the averaged energy per bit, denoted by E_b, to the power spectral density of the AWGN, denoted by N_0.

3.1. Slow fading channel

The average BER of the non-adaptive iterative MMSE receiver for various numbers of iterations under the perfect channel knowledge assumption is shown in Fig. 3. The system performance is significantly improved for the second iteration compared to the first iteration and gradually increases for higher iterations. The BER curves also

show that the performance converges to a steady state after the 3rd iteration. The performance of the adaptive iterative receiver based on the LMS algorithm and the non-adaptive iterative MMSE receiver are shown in Fig. 3.

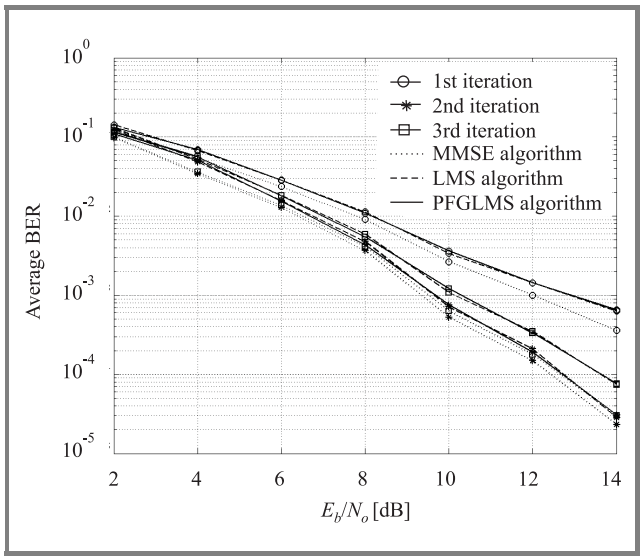


Fig. 3. Performance between the non-adaptive iterative MMSE algorithm and adaptive (LMS and PFGLMS) iterative algorithm in a quasi-static Rayleigh fading channel.

The results show that the average BER of the adaptive iterative structure approaches the performance results of the non-adaptive iterative MMSE receiver.

Figure 4 presents a comparison of the convergence speeds of the LMS and PFGLMS receiver at the 1st iteration. The figure shows that the convergence speed of the PFGLMS receiver outperforms that of the conventional LMS receiver.

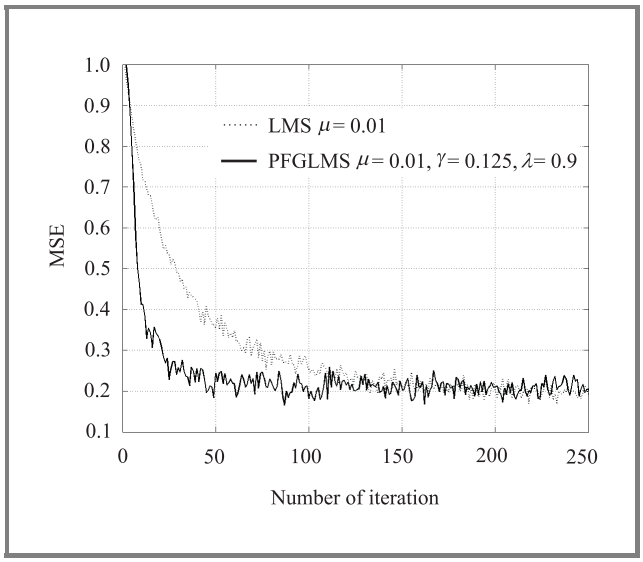


Fig. 4. The convergence speed of the conventional LMS and PFGLMS algorithm at $E_b/N_0 = 10$ dB.

The convergence rate of PFGLMS algorithm is about three times faster than that of the conventional LMS algorithm. However, the average BER of both structures is the same, as the average mean square error of the receivers is the same in a quasi-static fading channel.

3.2. Fast fading channel

The performance of the proposed receiver with the perfect knowledge of CSI at various fading rates is shown in Fig. 5. The figure shows that the average BER decreases when the fading rate is increased, since the MAP decoder performance is sensitive to the fade rates. When the fade

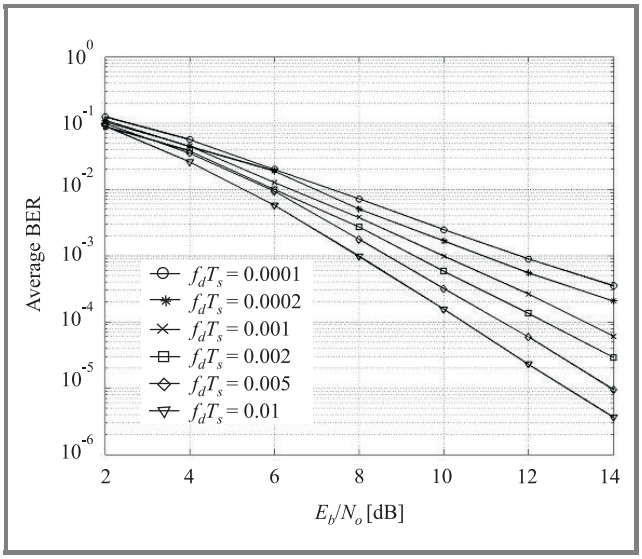


Fig. 5. Performance of the non-adaptive iterative MMSE receiver in various normalized fading rate with perfect channel knowledge.

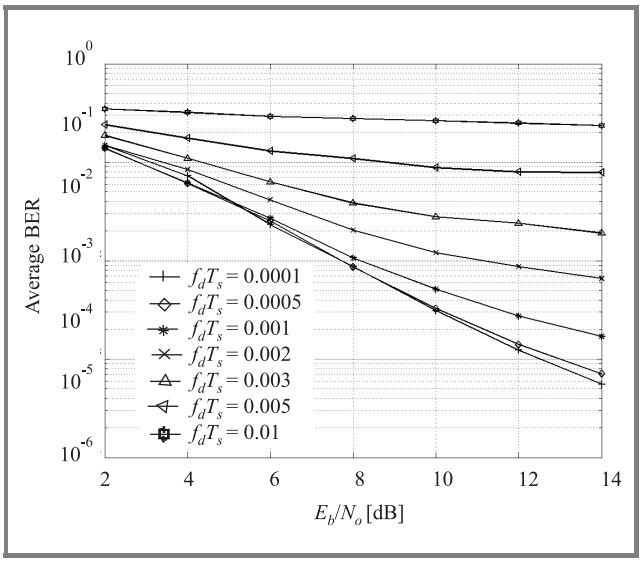


Fig. 6. Performance of the LMS adaptive iterative receiver in various normalized fading rate with imperfect channel knowledge.

rate is increased the inputs to the MAP decoder are less correlated and the decoder has a better performance. On the other hand, the LMS adaptive detector is sensitive to the channel estimation accuracy [11]. Therefore the average BER of the LMS adaptive iterative receiver is increased because of inaccurate channel estimation in fast fading channel. Therefore, the average BER of the LMS receiver increases when the fade rate is increased as shown in Fig. 6.

Figure 7 presents the comparison of the MMSE, LMS and PFGLMS receivers at the normalized fading rate of 0.0002.

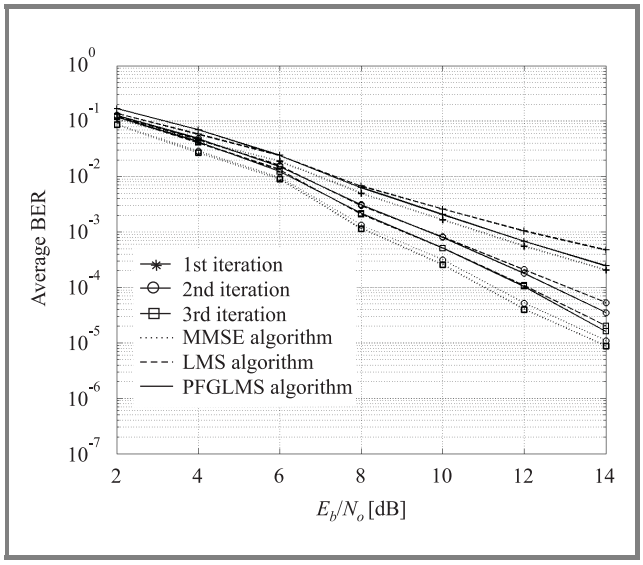


Fig. 7. Comparison between the non-adaptive iterative MMSE algorithm and adaptive (LMS and PFGLMS) iterative algorithm at the 0.0002 normalizes fading rate.

The result shows that the PFGLMS algorithm has a good tracking ability compared to the LMS algorithm on a fast fading channel. The average BER of the PFGLMS receiver is close to the average BER of MMSE receiver in the first iteration. Therefore, the PFGLMS receiver is more convenient for the fast fading channels.

4. Conclusion

A new adaptive iterative receiver for MIMO systems has been developed based on a joint adaptive iterative detection and decoding structure. The adaptive iterative receiver reduces co-channel interference by interference suppression and cancellation techniques. The comparison of the complexity is also consider only in the detector. The complexity of the proposed receiver is lower than that of the non-adaptive receiver because there is no matrix inversion. The complexity is reduced from the order of M^3 in non-adaptive receiver to the order of M in adaptive receiver in each received data symbol. However, there is a need for transmission of training sequences at the beginning of each simulation. Moreover, the proposed receiver based on the PFGLMS algorithm has a faster convergence speed and better tracking ability compared to the LMS receiver in fast fading channels with a slight increase in the complexity in term of the number of multiplier and adder. Therefore the PFGLMS receiver needs a shorter trainning period than that of LMS receiver. The performance of the proposed receiver approaches the one of non-adaptive iterative receiver.

References

[1] E. Telatar, "Capacity of multiantenna Gaussian channels", AT&T-Bell Labs., Internal. Tech. Memo., 1995.

[2] G. J. Foschini and M. J. Gans, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas", *Bell Labs. Techn. J.*, vol. 1, pp. 41–59, 1996.

[3] H. El Gamal and A. R. Hammons, Jr., "A new approach to layered space-time coding and signal processing", *IEEE Trans. Inform. Theory*, vol. 47, pp. 2321–2334, 2001.

[4] S. Marinkovic, B. Vucetic, and A. Ushirokawa, "Space-time iterative and multistage receiver structures for CDMA mobile communication systems", *IEEE J. Select. Areas Commun.*, vol. 19, pp. 1594–1604, 2001.

[5] J. Li, K. B. Letaief, and Z. Cao, "Adaptive co-channel interference cancellation in space-time coded communication systems", *IEEE Trans. Commun.*, vol. 50, pp. 1580–1583, 2002.

[6] H. El Gamal and E. Geraniotis, "Iterative multiuser detection for coded CDMA signals in AWGN and fading channels", *IEEE J. Select. Areas Commun.*, vol. 18, pp. 30–41, 2000.

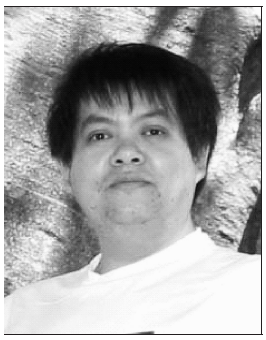
[7] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 3rd ed. Baltimore: Johns Hopkins University Press, 1996.

[8] S. S. Haykin, *Adaptive Filter Theory*, 4th ed. Upper Saddle River: Prentice Hall, 2002.

[9] J. S. Lim, "Fast adaptive filtering algorithm based on exponentially weighted least-square errors", *Electron. Lett.*, vol. 35, no. 22, pp. 1913–1915, 1999.

[10] S. Marinkovic, "Interference mitigation in CDMA and space-time coded MIMO systems", Ph.D. thesis, Telecommunications Laboratory, Department of Electrical and Information Engineering, University of Sydney, 2002.

[11] M. Stojanovic, J. G. Proakis, and J. A. Catipovic, "Analysis of the impact of channel estimation errors on the performance of a decision-feedback equalizer in fading multipath channels", *IEEE Trans. Commun.*, vol. 43, pp. 877–886, 1995.



Chakree Teekapakvisit was born in Surat Thani, Thailand, in 1968. He received the B.S. degree in electronic technology from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 1990 and the M.S. degree from the School of Electrical and Information Engineering, the University of Sydney in 2000. He is currently working towards the Ph.D. degree at The University of Sydney, Sydney, Australia. His research interests

include wireless communication, adaptive signal processing, multiple-input multiple-output (MIMO) system, space-time coding techniques and multiuser receivers for CDMA system.

e-mail: teekapak@ee.usyd.edu.au
School of Electrical and Information Engineering
The University of Sydney
Sydney, NSW 2006, Australia

Van Dong Pham received the B.E. degree from the University of South Australia in 1992, M.E.S. and Ph.D. degrees from the University of New South Wales, in 1995 and 2000, respectively. He is currently with the Department of Electrical and Information Engineering, The University of Sydney, Australia. His research interests include wireless communications, adaptive arrays, adaptive signal processing, and multiuser receivers for CDMA.

e-mail: vpham@ee.usyd.edu.au
School of Electrical and Information Engineering
The University of Sydney
Sydney, NSW 2006, Australia

Branka Vucetic received the B.S.E.E., M.S.E.E. and Ph.D. degrees in 1972, 1978 and 1982, respectively, in electrical engineering, from The University of Belgrade, Belgrade. During her career she has held various research and academic positions in Yugoslavia, Australia and UK. Since 1986 she has been with The University of Sydney, School of Electrical and Information Engineering, Australia. She is currently the Head of the School of Electrical and Information Engineering and the Director of The Telecommunications Laboratory at The University of Sydney. Her research interests include wireless communications, digital communication theory, coding and multiuser detection. In the past decade, she has been working on a number of industry-sponsored projects in wireless communications and mobile Internet. She has taught a wide range of undergraduate, postgraduate and continuing education courses worldwide. Professor Vucetic published four books and more than two hundred papers in telecommunications journals and conference proceedings.

e-mail: branka@ee.usyd.edu.au
School of Electrical and Information Engineering
The University of Sydney
Sydney, NSW 2006, Australia

Paper

Exact pairwise error probability analysis of space-time codes in spatially correlated fading channels

Tharaka A. Lamahewa, Marvin K. Simon, Thushara D. Abhayapala, and Rodney A. Kennedy

Abstract—In this paper, we derive an analytical expression for the exact pairwise error probability (PEP) of a space-time coded system operating over a spatially correlated slow fading channel using a moment-generating function-based approach. This analytical PEP expression is more realistic than previously published exact-PEP expressions as it fully accounts for antenna spacing, antenna geometries (uniform linear array, uniform grid array, uniform circular array, etc.) and scattering models (uniform, Gaussian, Laplacian, Von-Mises, etc.). Inclusion of spatial information provides valuable insights into the physical factors determining the performance of a space-time code. We demonstrate the strength of our new analytical PEP expression by evaluating the performance of two space-time trellis codes proposed in the literature for different spatial scenarios.

Keywords— Gaussian Q-function, modal correlation, moment-generating function, MIMO system, non-isotropic scattering, space-time coding.

1. Introduction

Space-time coding combines channel coding with multiple transmit and multiple receive antennas to achieve bandwidth and power efficient high data rate transmission over fading channels. The performance criteria for space-time codes have been derived in [1] based on the Chernoff bound applied to the pairwise error probability (PEP). In general, the Chernoff bound is quite loose for low signal-to-noise ratios. In [2], the exact-PEP of space-time codes operating over independent and identically distributed (i.i.d.) fast fading channels was derived using the method of residues. A simple method for exactly evaluating the PEP based on the moment generating function associated with a quadratic form of a complex Gaussian random variable [3] is given in [4] for both i.i.d. slow and fast fading channels. The fading correlation effects on the performance of space-time codes were investigated in [5]. There, the exact-PEP results derived in [2] were further extended to spatially correlated slow fading channels with the use of residue methods. In [5], the correlation is calculated in terms of the correlation between channel gains, but there is no direct realizable physical interpretation to the spatial correlation. Therefore, existing PEP expressions derived in the literature do not provide insights into the physical factors determining the performance of a space-time code operating over correlated fading channels. In particular, the effect of antenna spacing, spatial geometry of the antenna arrays and the non-isotropic scattering environments on the performance of space-time codes are of interest.

In this paper, using the MGF-based approach presented in [4], we derive an analytical expression for the exact-PEP of a space-time coded system operating over a spatially correlated slow fading channel. This expression is more realistic than previously published exact-PEP expressions, as it fully accounts for antenna placement along with non-isotropic scattering environments. In this work, we use a recently developed novel spatial channel model [6, 7] to incorporate the above factors in to the exact-PEP expression of a space-time coded system. Using this analytical exact-PEP expression, one can evaluate the performance of a space-time code applied to a MIMO system in any general spatial scenario (*antenna geometries*: uniform linear array (ULA), uniform grid array (UGA), uniform circular array (UCA), etc., *scattering models*: uniform, Gaussian, Laplacian, Von-Mises, etc.) without the need for extensive simulations. We provide an analytical technique which can be used to evaluate the exact-PEP in closed form. The strength of our new analytical exact-PEP expression is demonstrated by evaluating the performance of a 4-state QPSK space-time trellis code with two transmit antennas proposed by Tarokh *et al.* [1] and a 16-state QPSK space-time trellis code with three transmit antennas proposed by Zuho-Chen *et al.* [8] for different spatial scenarios.

The rest of this paper is organized as follows. Section 2 reviews the spatial channel model derived in [6]. Section 3 formulates the exact-PEP of a space-time coded system operating over a spatially correlated channel and Section 4 discusses a technique which can be used to obtain analytical solutions for the exact-PEP. Section 5 is devoted to examples, where we investigate the effects of antenna spacing, antenna configuration and scattering channel correlation for two space-time trellis codes. Finally, conclusions are drawn in Section 6.

Notations. Throughout the paper, the following notations will be used: $[\cdot]^T$, $[\cdot]^*$ and $[\cdot]^\dagger$ denote the transpose, complex conjugate and conjugate transpose operations, respectively. The symbols $\delta(\cdot)$ and $\otimes$ denote the Dirac delta function and matrix Kronecker product, respectively. The notation $E\{\cdot\}$ denotes the mathematical expectation, $\mathrm{Q}(y) = \frac{1}{\sqrt{2\pi}} \int_y^\infty e^{-x^2/2} dx$ denotes the Gaussian Q-function, $\mathrm{vec}(A)$ denotes the vectorization operator which stacks the columns of A, and $\lceil . \rceil$ denotes the ceiling operator. The matrix I_n is the $n \times n$ identity matrix.

2. System model

Consider a multi input multi output (MIMO) system consisting of n_T transmit antennas and n_R receive antennas. Let $x_n = [x_1^{(n)}, x_2^{(n)}, \cdots x_{n_T}^{(n)}]^T$ denote the space-time coded signal vector transmitted from n_T transmit antennas in the nth symbol interval and $X = [x_1, x_2, \cdots, x_L]$ denote the space-time code representing the entire transmitted signal, where L is the code length. Assuming quasi-static fading, the signals received at n_R receiver antennas during L symbol periods can be expressed in matrix form as

$$Y = \sqrt{E_s}HX + N,$$

where E_s is the transmitted power per symbol at each transmit antenna and H is the $n_R \times n_T$ zero-mean complex valued channel gain matrix, N is the noise represented by an $n_R \times L$ complex matrix in which entries are zero-mean independent Gaussian distributed random variables with variance $N_0/2$ per dimension.

Spatial channel model. Using a recently developed spatial channel model [6], we are able to incorporate the antenna spacing, antenna placement and scattering distribution parameters such as mean angle-of-arrival (AOA), mean angle-of-departure (AOD) and angular spread, into the exact-PEP calculations of space-time coded systems. In this spatial channel model, MIMO channel is separated in to three physical regions of interest: scatterer free region around the transmitter antenna array, scatterer free region around the receiver antenna array and the complex random scattering media which is the complement of the unions of two antenna array regions. In other words, MIMO channel is decomposed into deterministic and random matrices, where the deterministic portion depends on the physical configuration of the transmitter and the receiver antenna arrays and the random portion represents the complex scattering media between the transmitter and the receiver antenna regions.

Let u_p, $p = 1, 2, \cdots, n_T$ be the position of pth transmit antenna relative to the transmitter antenna array origin and v_q, $q = 1, 2, \cdots, n_R$ be the position of qth receive antenna relative to the receiver antenna array origin. Assume that the scatterers are distributed in the farfield from the transmitter and the receiver antenna arrays and the two regions are distinct. Then the MIMO channel H has the decomposition

$$H = J_R H_S J_T^{\dagger}, \tag{1}$$

where J_R is the $n_R \times (2m_R + 1)$ receiver antenna array configuration matrix,

$$J_R = \begin{pmatrix} \mathscr{J}_{-m_R}(v_1) & \cdots & \mathscr{J}_{m_R}(v_1) \\ \mathscr{J}_{-m_R}(v_2) & \cdots & \mathscr{J}_{m_R}(v_2) \\ \vdots & \ddots & \vdots \\ \mathscr{J}_{-m_R}(v_{n_R}) & \cdots & \mathscr{J}_{m_R}(v_{n_R}) \end{pmatrix},$$

J_T is the $n_T \times (2m_T + 1)$ transmitter antenna array configuration matrix,

$$J_T = \begin{pmatrix} \mathscr{J}_{-m_T}(u_1) & \cdots & \mathscr{J}_{m_T}(u_1) \\ \mathscr{J}_{-m_T}(u_2) & \cdots & \mathscr{J}_{m_T}(u_2) \\ \vdots & \ddots & \vdots \\ \mathscr{J}_{-m_T}(u_{n_T}) & \cdots & \mathscr{J}_{m_T}(u_{n_T}) \end{pmatrix},$$

with $\mathscr{J}_n(x)$ defined as the spatial-to-mode function (SMF) which maps the antenna location to the nth mode of the region. The form which the SMF takes is related to the shape of the scatterer-free antenna region. For a circular region in 2-dimensional space, the SMF is given by a Bessel function of the first kind [6] and for a spherical region in 3-dimensional space, the SMF is given by a spherical Bessel function [7]. For a prism-shaped region, the SMF is given by a prolate spheroidal function [9]. Here, we consider only the 2-dimensional[1] scattering environment where antennas are encompassed in scatterer-free circular apertures. In this case, SMF is given by

$$\mathscr{J}_n(w) = J_n(k\|w\|)\mathrm{e}^{in(\phi_w - \pi/2)},$$

where $J_n(\cdot)$ is the Bessel function of integer order n, vector $w = (\|w\|, \phi_w)$ in polar coordinates is the antenna location relative to the origin of the aperture which encloses the antennas, $k = 2\pi/\lambda$ is the wave number with λ being the wave length and $i = \sqrt{-1}$. $M_T = (2m_T + 1)$ and $M_R = (2m_R + 1)$ are the number of effective communication modes[2] available in the transmitter and receiver regions, respectively. Note that, m_T and m_R are determined by the size of the antenna aperture, but not from the number of antennas encompassed in an antenna array. The number of effective communication modes (M) available in a region is given by [10]

$$M = 2\lceil \pi e r/\lambda \rceil + 1, \tag{2}$$

where r is the minimum radius of the antenna array aperture and $\mathrm{e} \approx 2.7183$. H_S in Eq. (1) is the $(2m_R + 1) \times (2m_T + 1)$ random scattering matrix with (ℓ, m)th element given by

$$\{H_S\}_{\ell,m} = \int_0^{\pi}\int_0^{\pi} g(\phi, \varphi)\mathrm{e}^{-i(\ell - m_R - 1)\varphi}\mathrm{e}^{i(m - m_T - 1)\phi} d\varphi d\phi,$$
$$\ell = 1, \cdots, 2m_R + 1, \quad m = 1, \cdots, 2m_T + 1. \tag{3}$$

Note that $\{H_S\}_{\ell,m}$ represents the complex gain of the scattering channel between the mth mode of the transmitter region and the ℓth mode of the receiver region, where $g(\phi, \varphi)$ is the scattering gain function, which is the effective random complex gain for signals leaving the transmitter aperture with angle of departure ϕ and arriving at the receiver aperture with angle of arrival φ.

[1] The 2D case is a special case of the 3D case where all the signals arrive from on a horizontal plane only. Similar results can be obtained using the 3D channel model proposed in [7].

[2] The set of modes form a basis of functions for representing a multipath wave field.

3. Exact PEP on correlated MIMO channels

Assume that perfect channel state information (CSI) is available at the receiver and also a maximum likelihood (ML) decoder is employed at the receiver. Assume that the codeword X was transmitted, but the ML-decoder chooses another codeword $\hat{X}$. Then the PEP, conditioned on the channel, is given by [1]

$$\mathrm{P}(X \to \hat{X}|h) = \mathrm{Q}\left(\sqrt{\frac{E_s}{2N_0} d^2(X,\hat{X})}\right), \tag{4}$$

where $d^2(X,\hat{X}) = h[I_{n_R} \otimes X_\Delta]h^\dagger$, $X_\Delta = (X-\hat{X})(X-\hat{X})^\dagger$, $h = (\mathrm{vec}\,(H^T))^T$ is a row vector. To compute the average PEP, we average Eq. (4) over the joint probability distribution of h. By using Craig's formula for the Gaussian Q-function [11, Chap. 4, Eq. (4.2)]

$$\mathrm{Q}(x) = \frac{1}{\pi}\int_0^{\pi/2} \exp\left(-\frac{x^2}{2\sin^2\theta}\right) d\theta$$

and the MGF-based technique presented in [4], we can write the average PEP as

$$\begin{aligned}\mathrm{P}(X \to \hat{X}) &= \frac{1}{\pi}\int_0^{\pi/2}\int_0^{\infty} \exp\left(-\frac{\Gamma}{2\sin^2\theta}\right) p_\Gamma(\Gamma) d\Gamma d\theta, \\ &= \frac{1}{\pi}\int_0^{\pi/2} \mathscr{M}_\Gamma\left(-\frac{1}{2\sin^2\theta}\right) d\theta, \end{aligned} \tag{5}$$

where $\mathscr{M}_\Gamma(s) = \int_0^\infty \mathrm{e}^{s\Gamma} p_\Gamma(\Gamma) d\Gamma$ is the MGF of

$$\Gamma = \frac{E_s}{2N_0} h[I_{n_R} \otimes X_\Delta]h^\dagger \tag{6}$$

and $p_\Gamma(\Gamma)$ is the probability density function (pdf) of Γ. Substituting Eq. (1) for H in $h = (\mathrm{vec}\,(H^T))^T$ and using the Kronecker product identity [12, p. 180] $\mathrm{vec}(AXB) = (B^T \otimes A)\,\mathrm{vec}\,(X)$, we rewrite Eq. (6) as

$$\Gamma = \frac{E_s}{2N_0} h_S (J_R^T \otimes J_T^\dagger)(I_{n_R} \otimes X_\Delta)(J_R^* \otimes J_T) h_S^\dagger \tag{7a}$$

$$= \frac{E_s}{2N_0} h_S \left[(J_R^\dagger J_R)^T \otimes (J_T^\dagger X_\Delta J_T)\right] h_S^\dagger \tag{7b}$$

$$= \frac{E_s}{2N_0} h_S G h_S^\dagger, \tag{7c}$$

where $h_S = (\mathrm{vec}(H_S{}^T))^T$ is a row vector and

$$G = (J_R^\dagger J_R)^T \otimes (J_T^\dagger X_\Delta J_T). \tag{8}$$

Note that, Eq. (7b) follows from Eq. (7a) via the identity [12, p. 180] $(A \otimes C)(B \otimes D) = AB \otimes CD$, provided that the matrix products AB and CD exist.

Note that $h_S G h_S^\dagger$ in Eq. (7c) is a quadratic form of a random variable since h_S is a random row vector and G is fixed as J_T, J_R and X_Δ are deterministic matrices. Furthermore, the matrix G is Hermitian as both $J_R^\dagger J_R$ and $J_T^\dagger X_\Delta J_T$ are Hermitian, and the Kronecker product between two Hermitian matrices is always Hermitian. The MGF associated with a quadratic random variable is readily found in the literature [3]. Using [3, Eq. (14)], we write the MGF of Γ as

$$\mathscr{M}_\Gamma(s) = \left[\det\left(I - \frac{s\bar{\gamma}}{2} RG\right)\right]^{-1}, \tag{9}$$

where $\bar{\gamma} = \frac{E_s}{N_0}$ is the average symbol energy-to-noise ratio (SNR) and $R = E\left\{h_S^\dagger h_S\right\}$ is the covariance matrix of h_S. Here we assumed that the entries of h_S are zero-mean complex Gaussian distributed.

Substitution of Eq. (9) into Eq. (5) gives the exact-PEP

$$\mathrm{P}(X \to \hat{X}) = \frac{1}{\pi}\int_0^{\pi/2} \left[\det\left(I + \frac{\bar{\gamma}}{4\sin^2\theta} RG\right)\right]^{-1} d\theta. \tag{10}$$

Remark 1: Equation (10) is the exact-PEP[3] of a space-time coded system applied to a spatially correlated slow fading MIMO channel following the channel decomposition in Eq. (1).

Remark 2: When $R = I$ (i.e., correlation between different communication modes is zero), Eq. (10) above captures the effects due to antenna spacing and antenna geometry on the performance of a space-time code operating over a slow fading channel.

Remark 3: When the fading channels are independent (i.e., $R = I$ and $G = I_{n_R} \otimes X_\Delta$), Eq. (10) simplifies to,

$$\mathrm{P}(X \to \hat{X}) = \frac{1}{\pi}\int_0^{\pi/2} \left[\det\left(I_{n_T} + \frac{\bar{\gamma}}{4\sin^2\theta} X_\Delta\right)\right]^{-n_R} d\theta,$$

which is the same as [4, Eq. (13)].

Kronecker product model as a special case. In some circumstances, the covariance matrix R of the scattering channel H_S can be expressed as a Kronecker product between correlation matrices observed at the receiver and the transmitter antenna arrays [13, 14], i.e.,

$$R = E\left\{h_S^\dagger h_S\right\} = F_R \otimes F_T, \tag{11}$$

where F_R and F_T are the transmit and receive correlation matrices. Substituting Eq. (11) in Eq. (10) and recalling the definition of G in Eq. (8), the exact-PEP can be written as

$$\mathrm{P}(X \to \hat{X}) = \frac{1}{\pi}\int_0^{\pi/2} \left[\det\left(I + \frac{\bar{\gamma}}{4\sin^2\theta} Z\right)\right]^{-1} d\theta\,, \tag{12}$$

where $Z = (F_R J_R^T J_R^*) \otimes (F_T J_T^\dagger X_\Delta J_T)$.

[3]Equation (10) can be evaluated in closed form using the analytical technique discussed in Section 4.

4. Realistic exact-PEP

The exact-PEP expression we derived in the previous section captures the antenna configurations (linear array, circular array, grid, etc.) both at the transmitter and the receiver arrays via J_T and J_R, respectively. Furthermore, it also incorporates the modal correlation effects at the transmitter and the receiver regions via F_T and F_R, respectively. Therefore, the PEP expression Eq. (12) can be considered as the *realistic* exact PEP of a space-time coded system.

To calculate the exact-PEP, one needs to evaluate the integral Eq. (12) (or Eq. (10) in a more general spatial scenario), either using numerical methods or analytical methods. We present an analytical technique which can be employed to evaluate the integral Eq. (12) in closed form as follows.

Matrix Z in Eq. (12) has size $M_R M_T \times M_R M_T$. Therefore, the integrand in Eq. (12) will take the form[4]

$$\left[\det\left(I+\frac{\bar{\gamma}}{4\sin^2\theta}Z\right)\right]^{-1}=\frac{(\sin^2\theta)^N}{\sum_{\ell=0}^{N}a_\ell(\sin^2\theta)^\ell}, \tag{13}$$

where $N=M_RM_T$ and a_ℓ, for $\ell=1,2,\cdots,N$, are constants. Note that the denominator of Eq. (13) is an Nth order polynomial in $\sin^2\theta$. To evaluate the integral Eq. (13) in closed form, we use the partial-fraction expansion technique given in [11, Appendix 5A] as follows.

First we begin by factoring the denominator of Eq. (13) into terms of the form $(\sin^2\theta+c_\ell)$, for $\ell=1,2,\cdots,N$. This involves finding the roots of an Nth order polynomial in $\sin^2\theta$ either numerically or analytically. Then Eq. (13) can be expressed in product form as

$$\frac{(\sin^2\theta)^N}{\sum_{\ell=0}^{N}a_\ell(\sin^2\theta)^\ell}=\prod_{\ell=1}^{\Lambda}\left(\frac{\sin^2\theta}{c_\ell+\sin^2\theta}\right)^{m_\ell}, \tag{14}$$

where m_ℓ is the multiplicity of the root c_ℓ and $\sum_{\ell=1}^{\Lambda}m_\ell=N$. Applying the partial-fraction decomposition theorem to the product form Eq. (14), we get

$$\prod_{\ell=1}^{\Lambda}\left(\frac{\sin^2\theta}{c_\ell+\sin^2\theta}\right)^{m_\ell}=\sum_{\ell=1}^{\Lambda}\sum_{k=1}^{m_\ell}A_{k\ell}\left(\frac{\sin^2\theta}{c_\ell+\sin^2\theta}\right)^{k}, \tag{15}$$

where the residual $A_{k\ell}$ is given by [11, Eq. (5A.72)]

$$A_{k\ell}=\frac{\left\{\frac{d^{m_\ell-k}}{dx^{m_\ell-k}}\prod_{\substack{n=1\\n\neq\ell}}^{\Lambda}\left(\frac{1}{1+c_nx}\right)^{m_n}\right\}|_{x=-c_\ell^{-1}}}{(m_\ell-k)!c_\ell^{m_\ell-k}}. \tag{16}$$

Expansion Eq. (15) often allows integration to be performed on each term separately by inspection. In fact, each term in Eq. (15) can be separately integrated using a result found in [4], where

$$\begin{aligned}P(c_\ell,k)&=\frac{1}{\pi}\int_0^{\pi/2}\left(\frac{\sin^2\theta}{c_\ell+\sin^2\theta}\right)^k d\theta,\\&=\frac{1}{2}\left[1-\sqrt{\frac{c_\ell}{1+c_\ell}}\sum_{j=0}^{k-1}\binom{2j}{j}\left(\frac{1}{4(1+c_\ell)}\right)^j\right].\end{aligned} \tag{17}$$

Now using the partial-fraction form of the integrand in Eq. (15) together with Eq. (17), we obtain the exact-PEP in closed form as

$$\begin{aligned}\mathrm{P}(X\to\hat{X})&=\frac{1}{\pi}\int_0^{\pi/2}\prod_{k=1}^{\Lambda}\left(\frac{\sin^2\theta}{c_\ell+\sin^2\theta}\right)^{m_\ell}d\theta,\\&=\sum_{\ell=1}^{\Lambda}\sum_{k=1}^{m_\ell}A_{k\ell}P(c_\ell,k).\end{aligned} \tag{18}$$

For the special case of distinct roots, i.e., $m_1=m_2=\cdots=m_N=1$, the exact-PEP is given by

$$\mathrm{P}(X\to\hat{X})=\frac{1}{2}\sum_{\ell=1}^{N}\left(1-\sqrt{\frac{c_\ell}{1+c_\ell}}\right)\prod_{\substack{n=1\\n\neq\ell}}^{N}\left(\frac{c_\ell}{c_\ell-c_n}\right).$$

5. Analytical performance evaluation: examples

In this section, we consider the following two space-time codes as examples:

- 4-state QPSK space-time trellis code with two transmit antennas [1, Fig. 4]; the shortest error event path of length 2, as illustrated by shading in Fig. 1 of [4];
- 16-state QPSK space-time trellis code with three transmit antennas [8, Table 1]; the shortest error event path of length 3.

For the 4-state code, the exact-PEP results and approximate bit error probability (BEP) results for $n_R=1$ and $n_R=2$ were presented in [2, 4] for i.i.d. fast fading and slow fading channels. In [5], the effects of fading correlation on the average BEP were studied for $n_R=1$ over a slow fading channel. In this work, we compare the i.i.d. channel performance results presented in [2, 4] with our realistic exact-PEP results for different antenna spacing and scattering distribution parameters. In addition, we use the 16-state code with three transmit antennas to study the impact of antenna placement on the performance of space-time codes.

In [2, 4], performances were evaluated under the assumption that the transmitted codeword is the all-zero codeword. Here we also adopt the same assumption as we compare our results with their results. However, we are aware that space-time codes may, in general, be nonlinear, i.e., the average BEP can depend on the transmitted codeword.

[4] One would need to evaluate the determinant of $\left(I+\frac{\bar{\gamma}}{4\sin^2\theta}Z\right)$ and then take the reciprocal of it to obtain the form Eq. (13).

5.1. Effect of antenna spacing

First we consider the effect of antenna spacing on the exact-PEP when the scattering environment is isotropic, i.e., $F_T = I_{2m_T+1}$ and $F_R = I_{2m_R+1}$. Consider the 4-state code with two transmit antennas and two receive antennas, where the two transmit antennas are placed in a circular aperture of radius 0.25λ (antenna separation[5] = 0.5λ) and the two receive antennas are placed in a circular aperture of radius r (antenna separation = $2r$).

Figure 1 shows the exact pairwise error probability performance of the 4-state code for length 2 error event and receive antenna separations 0.1λ, 0.2λ, 0.5λ and λ. Also shown in Fig. 1 for comparison is the exact-PEP for the i.i.d. slow fading channel (Rayleigh) corresponding to the length two error event path.

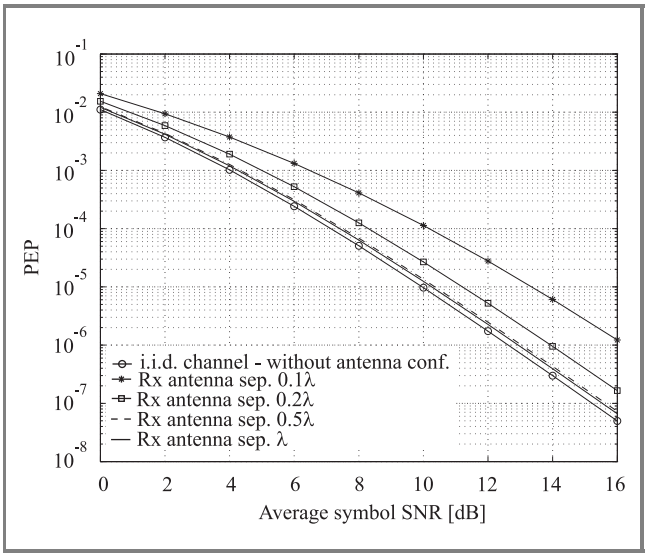


Fig. 1. Exact pairwise error probability performance of the 4-state space-time trellis code with 2-Tx antennas and 2-Rx antennas: length 2 error event.

As we can see from the figure, the effect of antenna separation on the exact-PEP is not significant when the receive antenna separation is 0.5λ or higher. However, the effect is significant when the receive antenna separation is small. For example, at PEP 10^{-5}, the realistic PEPs are 1 dB and 3 dB away from the i.i.d. channel performance results for 0.2λ and 0.1λ transmit antenna separations, respectively. From these observations, we can emphasize that the effect of antenna spacing on the performance of the 4-state code is minimum for higher antenna separations whereas the effect is significant for smaller antenna separations.

[5]In a 3D isotropic scattering environment, antenna separation 0.5λ (first null of the order zero spherical Bessel function) gives zero spatial correlation, but here we constraint our analysis to a 2D scattering environment. The spatial correlation function in a 2D isotropic scattering environment is given by a Bessel function of the first kind. Therefore, antenna separation $\lambda/2$ does not give zero spatial correlation in a 2D isotropic scattering environment.

5.2. Loss of diversity advantage due to a region with limited size

We now consider the diversity advantage of a space-time coded system as the number of receive antennas increases while the receive antenna array aperture radius remains fixed. Figure 2 shows the exact-PEP of the 4-state STTC

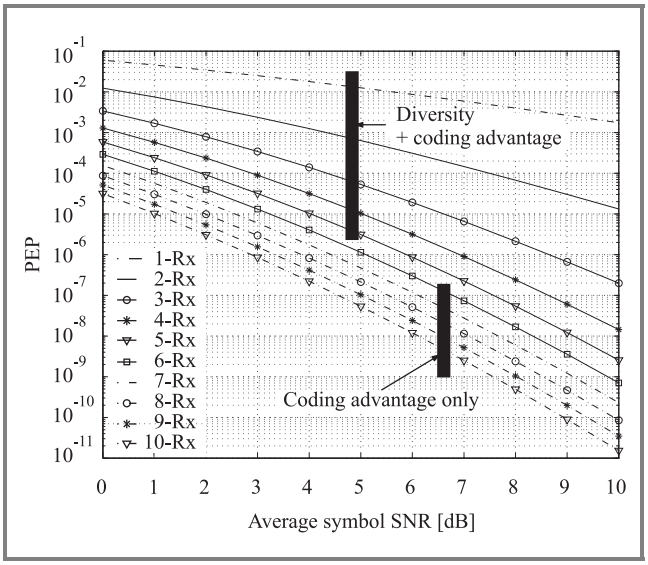


Fig. 2. Exact PEP performance of the 4-state space-time trellis code with 2-Tx antennas and n-Rx antennas: length 2 error event.

with two transmit antennas and n_R receive antennas, where $n_R = 1, 2, \ldots, 10$. The two transmit antennas are placed in a circular aperture of radius 0.25λ (antenna separation = 0.5λ) and n_R receive antennas are placed in a uniform circular array antenna configuration with radius 0.15λ. In this case, the distance between two adjacent receive antenna elements is $0.3\lambda \sin(\pi/n_R)$.

The slope of the performance curve on a log scale corresponds to the diversity advantage of the code and the horizontal shift in the performance curve corresponds to the coding advantage. According to the code construction criteria given in [1], the diversity advantage promised by the 4-state STTC is $2n_R$. With the above antenna configuration setup, however, we observed that the slope of each performance curve remains the same when $n_R > 5$, which results in zero diversity advantage improvement for $n_R > 5$. Nevertheless, for $n_R > 5$, we still observed some improvement in the coding gain, but the rate of improvement is slower with the increase in number of receive antennas. Here the loss of diversity gain is due to the fewer number of effective communication modes available at the receiver region than the number of antennas available for reception. In this case, from Eq. (2), the receive aperture of radius 0.15λ corresponds to $M = 2\lceil \pi e 0.15 \rceil + 1 = 5$ effective communication modes at the receive region. Therefore when $n_R > 5$, the diversity advantage of the code is determined by the number of effective communication modes available at the receiver

antenna region rather than the number of antennas available for reception. That is, the point where the diversity loss occurred is clearly related to the size of the antenna aperture, where smaller apertures result in diversity loss of the code for lower number of receive antennas, as proved analytically in [15].

5.3. Effect of antenna configuration

In this section, we compare the PEP performance of the 16-state code for different antenna configurations at the transmitter antenna array. Here we consider UCA and ULA antenna configurations as examples.[6] We place the three transmit antennas within a fixed circular aperture of radius $r(=0.15\lambda, 0.25\lambda)$, where the antenna placements are shown in Fig. 3. The exact-PEP performance for the error event path of length three is also shown in Fig. 3 for a single receive antenna.

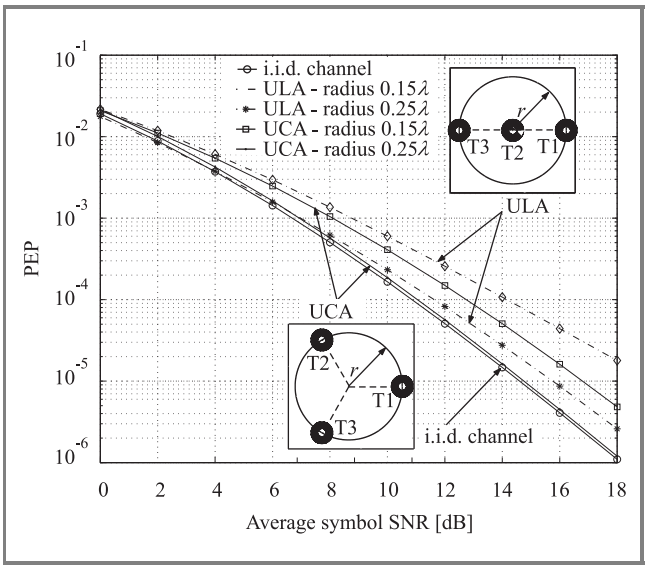


Fig. 3. The exact-PEP performance of the 16-state code with three transmit and one receive antennas for UCA and ULA transmit antenna configurations: length 3 error event.

From Fig. 3, it is observed that at high SNRs the performance given by the UCA antenna configuration outperforms that of the ULA antenna configuration. For example, at PEP 10^{-5}, the performance difference between UCA and ULA are 2.75 dB with 0.15λ receiver aperture radius and 1.25 dB with 0.25λ receiver aperture radius. From Fig. 3, we observed that as the radius of the transmitter aperture decreases the diversity advantage of the code is reduced, particularly for the ULA antenna configuration. Here, the loss of diversity advantage is mainly due to the loss of rank of J_T.

[6]The exact-PEP expression we derived in this work can be applied to any arbitrary antenna configuration.

5.4. Effect of modal correlation

For simplicity, here we only consider the modal correlation effects at the receiver region and assume that the effective communication modes available at the transmitter region are uncorrelated, i.e., $F_T = I_{2m_T+1}$. First, we derive the definition of modal correlation matrix F_R at the receiver region.

Using Eq. (3), we can define the modal correlation between complex scattering gains as

$$\gamma_{m,m'}^{\ell,\ell'} = E\left\{\{H_S\}_{\ell,m}\{H_S\}_{\ell',m'}^{*}\right\}.$$

Assume that the scattering from one direction is independent of that from another direction for both the receiver and the transmitter apertures. Then the second-order statistics of the scattering gain function $g(\phi,\varphi)$ can be defined as

$$E\left\{g(\phi,\varphi)g^{*}(\phi',\varphi')\right\} = G(\phi,\varphi)\delta(\phi-\phi')\delta(\varphi-\varphi'),$$

where $G(\phi,\varphi) = E\left\{|g(\phi,\varphi)|^2\right\}$ with normalization $\int\int G(\phi,\varphi)d\varphi d\phi = 1$. With the above assumption, the modal correlation coefficient, $\gamma_{m,m'}^{\ell,\ell'}$ can be simplified to

$$\gamma_{m,m'}^{\ell,\ell'} = \int\int G(\phi,\varphi)\mathrm{e}^{-i(\ell-\ell')\varphi}e^{i(m-m')\phi}d\varphi d\phi.$$

Then the correlation between the ℓth and ℓ'th modes at the receiver region due to the mth mode at the transmitter region is given by

$$\gamma_{\ell,\ell'}^{Rx} = \int \mathscr{P}_{Rx}(\varphi)\mathrm{e}^{-i(\ell-\ell')\varphi}d\varphi, \qquad (19)$$

where $\mathscr{P}_{Rx}(\varphi) = \int G(\phi,\varphi)d\phi$ is the normalized azimuth power distribution of the scatterers surrounding the receiver antenna region. Here we see that modal correlation at the receiver is independent of the mode selected from the transmitter region. Note that the (ℓ,ℓ')th element of F_R is given by Eq. (19) and F_R is a $(2m_R+1)\times(2m_R+1)$ matrix. Also note that $\mathscr{P}_{Rx}(\varphi)$ can be modeled using all common azimuth power distributions such as uniform, Gaussian, Laplacian, Von-Mises, polynomial, etc.

It was shown in [16] that all azimuth power distribution models give very similar correlation values for a given angular spread, especially for small antenna separations. Therefore, without loss of generality, we restrict our investigation only to the case of energy arriving uniformly over a limited angular spread σ around a mean AOA φ_0 (uniform limited azimuth power distribution). In this case, the modal correlation coefficient $\gamma_{\ell,\ell'}^{Rx}$ in the receiver region is given by

$$\gamma_{\ell,\ell'}^{Rx} = \mathrm{sinc}((\ell-\ell')\sigma)\mathrm{e}^{-i(\ell-\ell')\varphi_0}. \qquad (20)$$

Continuing the performance analysis, we now investigate the modal correlation effects on the performance of

the 4-state code with two transmit and two receive antennas. We place the two transmit antennas 0.5λ apart and also the two receive antennas 0.5λ apart.[7]

Figure 4 shows the exact-PEP performances of the 4-state code for various angular spreads $\sigma = \{5^\circ, 30^\circ, 45^\circ, 180^\circ\}$ about a mean AOA $\varphi_0 = 0^\circ$ from broadside, where the broadside angle is defined as the angle perpendicular to the line connecting the two antennas. Note that $\sigma = 180^\circ$ represents the isotropic scattering environment.

The exact-PEP performance for the i.i.d. slow fading channel (Rayleigh) is also plotted on the same graph for comparison.

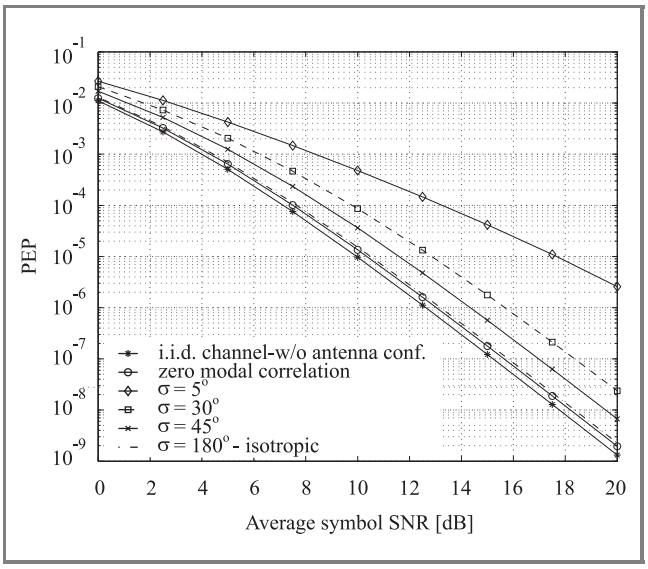


Fig. 4. Effect of receiver modal correlation on the exact-PEP of the 4-state QPSK space-time trellis code with 2-Tx antennas and 2-Rx antennas for the length 2 error event. Uniform limited power distribution with a mean angle of arrival $\varphi_0 = 0^\circ$ from broadside and angular spreads $\sigma = \{5^\circ, 30^\circ, 45^\circ, 180^\circ\}$.

As one would expect, the performance loss incurred due to the modal correlation increases as the angular spread of the distribution decreases.

For example, at PEP 10^{-5}, the realistic PEP results obtained from Eq. (12) are about 0.25 dB, 1.75 dB, 2.75 dB and 7.5 dB away from the i.i.d. channel performance results for angular spreads 180°, 45°, 30° and 5°, respectively. Therefore, in general, if the angular spread of the distribution is closer to 180° (isotropic scattering), then the loss incurred due to the modal correlation is insignificant, provided that the antenna spacing is optimal. However, for moderate angular spread values such as 45° and 30°, the performance loss is quite significant. This is due to the higher concentration of energy closer to the mean AOA for small angular spreads.

It is also observed that for large angular spread values, the diversity order of the code (the slope of the performance curve) is preserved whereas for small and moderate angular spread values, the diversity order of the code is diminished.

Figure 5 shows the PEP performance results of the 4-state code for a mean AOA $\varphi_0 = 60^\circ$ from broadside. Similar results are observed as for the mean AOA $\varphi_0 = 0^\circ$ case.

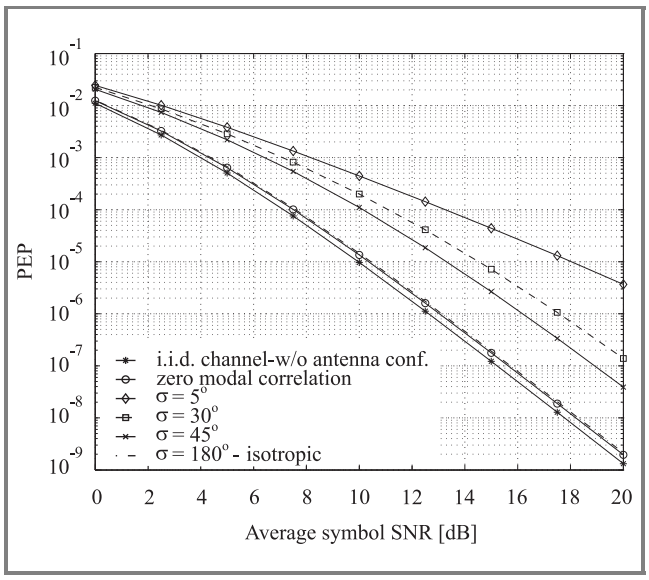


Fig. 5. Effect of receiver modal correlation on the exact-PEP of the 4-state QPSK space-time trellis code with 2-Tx antennas and 2-Rx antennas for the length 2 error event. Uniform limited power distribution with a mean angle of arrival $\varphi_0 = 60^\circ$ from broadside and angular spreads $\sigma = \{5^\circ, 30^\circ, 45^\circ, 180^\circ\}$.

Comparing Figs. 4 and 5 we observe that the performance loss is increased for all angular spreads as the mean AOA moves away from broadside. This can be justified by the reasoning that, as the mean AOA moves away from broadside, there will be a reduction in the angular spread exposed to the antennas and hence less signals being captured.

Furthermore, we observed that (performance results are not shown here) when there are more than two receive antennas in a fixed receiver aperture, the performance loss of the 4-state code with decreasing angular spread is most pronounced for the ULA antenna configuration when the mean AOA is closer to 90° (inline with the array). But, for the UCA antenna configuration, the performance loss is insignificant as the mean AOA moves away from broadside for all angular spreads. This suggests that the UCA antenna configuration is less sensitive to change of mean AOA compared to the ULA antenna configuration. Hence, the UCA antenna configuration is best suited to employ a space-time code.

Using the results we obtained thus far, we can claim that, in general, space-time trellis codes are susceptible to spatial fading correlation effects, in particular, when the antenna separation and the angular spread are small.

[7]Performance loss due to antenna spacing is minimum when the antenna separation is 0.5λ or higher as we showed in Subsection 5.1.

5.5. Extension of PEP to average bit error probability

An approximation to the average BEP was given in [17] on the basis of accounting for error event paths of lengths up to H as

$$P_b(E) \cong \frac{1}{b}\sum_t q(X \to \hat{X})_t P(X \to \hat{X})_t, \qquad (21)$$

where b is the number of input bits per transmission, $q(X \to \hat{X})_t$ is the number of bit errors associated with the error event t and $P(X \to \hat{X})_t$ is the corresponding PEP. In [4], it was shown that error event paths of lengths up to H are sufficient to achieve a reasonably good approximation to the full upper (union) bound that takes into account error event paths of all lengths. For example, with the 4-state STTC, error event paths of lengths up to $H = 4$ is sufficient for the slow fading channel.

The closed-form solution for average BEP of a space-time code can be obtained by finding closed-form solutions for PEPs associated with each error type, using the analytical technique given in Section 4. In previous sections, we investigate the effects of antenna spacing, antenna geometry and modal correlation on the exact-PEP of a space-time code over slow fading channel. The observations and claims which we made there, are also valid for the BEP case as the BEPs are calculated directly from PEPs. Therefore, to avoid repetition, we do not discuss BEP performance results here.

6. Conclusion

Using an MGF-based approach, we have derived an analytical expression for the exact pairwise error probability of a space-time coded system operating over a spatially correlated slow fading channel. This analytical PEP expression fully accounts for antenna separation, antenna geometry and surrounding azimuth power distributions, both at the receiver and the transmitter antenna arrays. In practice, it can be used as a tool to estimate or predict the performance of a space-time code under any antenna configuration and surrounding azimuth power distribution parameters. Based on this new PEP expression, we showed that space-time codes employed on multiple transmit and multiple receive antennas are susceptible to spatial fading correlation effects, particularly for small antenna separations and small angular spreads.

Acknowledgements

This work was supported by the Australian Research Council Discovery Grant DP0343804. Thushara D. Abhayapala is also with National ICT Australia, Locked Bag 8001, Canberra, ACT 2601, Australia. National ICT Australia is funded through the Australian Government's *Backing Australia's Ability* initiative, in part through the Australian Research Council.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction", *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 744–765, 1998.

[2] M. Uysal and C. N. Georghiades, "Error performance analysis of spacetime codes over Rayleigh fading channels", *J. Commun. Netw.*, vol. 2, no. 4, pp. 351–355, 2000.

[3] G. L. Turin, "The characteristic function of hermetian quadratic forms in complex normal random variables", *Biometrika*, vol. 47, no. 1–2, pp. 199–201, 1960.

[4] M. K. Simon, "Evaluation of average bit error probability for space-time coding based on a simpler exact evaluation of pairwise error probability", *Int. J. Commun. Netw.*, vol. 3, no. 3, pp. 257–264, 2001.

[5] M. Uysal and C. N. Georghiades, "Effect of spatial fading correlation on performance of space-time codes", *Electron. Lett.*, vol. 37, no. 3, pp. 181–183, 2001.

[6] T. D. Abhayapala, T. S. Pollock, and R. A. Kennedy, "Spatial decomposition of MIMO wireless channels", in *Proc. Seventh Int. Symp. Sig. Proces. Appl. ISSPA'2003*, Paris, France, 2003, vol. 1, pp. 309–312.

[7] T. D. Abhayapala, T. S. Pollock, and R. A. Kennedy, "Charakterization of 3D spatial wireless channels", in *IEEE Veh. Technol. Conf. (Fall) VTC 2003*, Orlando, USA, 2003.

[8] Z. Chen, B. Vucetic, J. Yuan, and K. L. Lo, "Space-time trellis codes with two, three and four transmit antennas in quasi-static flat fading channels", in *Proc. IEEE Int. Conf. Commun.*, New York, USA, 2002, pp. 1589–1595.

[9] L. Hanlen and M. Fu, "Wireless communications systems with spatial diversity: a volumetric approach", in *IEEE Int. Conf. Commun. ICC'2003*, Anchorage, USA, 2003, vol. 4, pp. 2673–2677.

[10] H. M. Jones, R. A. Kennedy, and T. D. Abhayapala, "On dimensionality of multipath fields: spatial extent and richness", in *Proc. IEEE Int. Conf. Acoust., Speech, Sig. Proces. ICASSP'2002*, Orlando, USA, 2002, vol. 3, pp. 2837–2840.

[11] M. K. Simon and M. S. Alouini, *Digital Communications over Fading Channels*, 2nd ed. Hoboken: Wiley, 2004.

[12] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 3rd ed. Baltimore, London: The Johns Hopkins University Press, 1996.

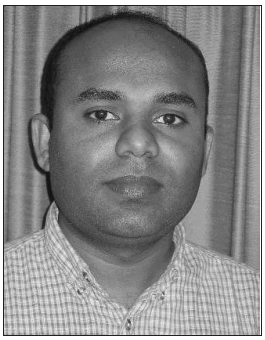
[13] J. P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation", *IEEE J. Selec. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, 2002.

[14] T. S. Pollock, "Correlation modelling in MIMO systems: when can we Kronecker?", in *Proc. 5th Austr. Commun. Theory Worksh.*, Newcastle, Australia, 2004, pp. 149–153.

[15] T. A. Lamahewa, R. A. Kennedy, and T. D. Abhayapala, "Upper-bound for the pairwise error probability of space-time codes in physical channel scenarios", in *Proc. 5th Austr. Commun. Theory Worksh.*, Brisbane, Australia, 2005, pp. 26–32.

[16] T. S. Pollock, T. D. Abhayapala, and R. A. Kennedy, "Introducing space into MIMO capacity calculations", *J. Telecommun. Syst.*, vol. 24, no. 2, pp. 415–436, 2003.

[17] J. K. Cavers and P. Ho, "Analysis of the error performance of trellis coded modulations in Rayleigh fading channels", *IEEE Trans. Commun.*, vol. 40, no. 1, pp. 74–83, 1992.



Tharaka A. Lamahewa received the B.E. (hons.) degree in information technology and telecommunications engineering from the University of Adelaide, South Australia, in 2000. He is currently pursuing the Ph.D. degree in telecommunications engineering at the Research School of Information Sciences and Engineering, Australian National University, Canberra. From 2001 to 2003, he worked as a software engineer at Motorola Electronics Pvt Ltd., Singapore. His research interests include space-time coding, MIMO channel modeling and MIMO capacity analysis for wireless communication systems.

e-mail: tharaka.lamahewa@anu.edu.au
Department of Information Engineering
Research School of Information Sciences and Engineering
The Australian National University
Canberra, ACT 0200, Australia

Marvin K. Simon is currently a Principal Scientist at the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, USA, where for the last 36 years he has performed research as applied to the design of NASA's deep-space and near-earth missions resulting in the issuance of 9 patents, 25 NASA Tech Briefs and 4 NASA Space Act awards. Doctor Simon is known as an internationally acclaimed authority on the subject of digital communications with particular emphasis in the disciplines of modulation and demodulation, synchronization techniques for space, satellite and radio communications, trellis-coded modulation, spread spectrum and multiple access communications, and communication over fading channels. He has published over 200 papers on the above subjects and is co-author of 11 textbooks. He is the co-recipient of the 1988 Prize Paper Award in Communications of the "IEEE Transactions on Vehicular Technology" for his work on trellis coded differential detection systems and also the 1999 Prize Paper of the IEEE Vehicular Technology Conference for his work on switched diversity. He is a Fellow of the IEEE and a Fellow of the IAE. Among his awards are the NASA Exceptional Service Medal, NASA Exceptional Engineering Achievement Medal, IEEE Edwin H. Armstrong Achievement Award and the IEEE Millennium Medal all in recognition of outstanding contributions to the field of digital communications and leadership in advancing this discipline.

e-mail: marvin.k.simon@jpl.nasa.gov
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA 91109, USA

Thushara D. Abhayapala was born in Colombo, Sri Lanka, in 1967. He received the B.E. degree in interdisciplinary systems engineering in 1994 and the Ph.D. degree in telecommunications engineering in 1999 from the Australian National University (ANU). From 1995 to 1997, he worked as a research engineer at the Arthur C. Clarke Centre for Modern Technologies, Sri Lanka. Since December 1999, Associate Professor Abhayapala has been with the Department of Information Engineering, Research School of Information Sciences and Engineering at the ANU. Currently he is a principal researcher and the program leader for Wireless Signal Processing program, National ICT Australia (NICTA), Canberra. His research interests are in the areas of space-time signal processing for wireless communication systems, spatio-temporal channel modeling, MIMO capacity analysis, UWB systems, array signal processing and acoustic signal processing. He has supervised 17 research students and co-authored approximately 100 papers. Doctor Abhayapala is currently an associate editor for EURASIP Journal on Wireless Communications and Networking.

e-mail: thushara.abhayapala@anu.edu.au.
Department of Information Engineering
Research School of Information Sciences and Engineering
The Australian National University
Canberra, ACT 0200, Australia

Rodney A. Kennedy has degrees from the University of New South Wales, Australia, University of Newcastle, and the Australian National University. He worked 3 years for CSIRO on the Australia Telescope Project. He is now with the Department of Information Engineering, Research School of Information Sciences and Engineering at the Australian National University. His research interests are in the fields of digital and wireless communications, digital signal processing and acoustical signal processing.

e-mail: rodney.kennedy@anu.edu.au
Department of Information Engineering
Research School of Information Sciences and Engineering
The Australian National University
Canberra, ACT 0200, Australia

Paper

CDMA wireless system with blind multiuser detector

Wai Yie Leong and John Homer

Abstract— In this paper we present an approach capable of countering the presence of multiple access interference (MAI) in code division multiple access (CDMA) channels. We develop and implement a blind multiuser detector, based on an independent component analysis (ICA) to mitigate both MAI and noise. This algorithm has been utilized in blind source separation (BSS) of unknown sources from their linear mixtures. It can also be used for estimation of the basis vectors of BSS. The aim is to include an ICA algorithm within a wireless receiver in order to reduce the level of interference in CDMA systems. This blind multiuser detector requires less precise knowledge of the channel than does the conventional single-user receiver. The proposed blind multiuser detector is made robust with respect to imprecise knowledge of the received signature waveforms of the user of interest. Several experiments are performed in order to verify the validity of the proposed learning algorithm.

Keywords— code division multiple access, independent component analysis, blind source separation.

1. Introduction

Code division multiple access (CDMA) multiuser detection has undergone rapid evolution through significant research and development activity in telecommunications [12, 13]. With the ever-growing sophistication of signal processing and computation, multiuser detection exploits the potential needs to increase capacity in multiuser radio channels. It deals with the demodulation of mutually interfering signals in applications such as cellular telephony, satellite communication and digital radio.

In general, multiuser detection is also known as cochannel interference suppression, multiuser demodulation, and interference cancellation to deal with the demodulation of digitally modulated signals in the presence of a multiaccess interference. Motivated by the channel environment encountered in many CDMA applications, the design of multiuser detectors for channels with fading, multipath, or noncoherent modulation has attracted considerable attention [6, 12]. An adaptive multiuser detector which converges to the minimum mean squared error (MMSE) detector without requiring training sequences is proposed in [6]. This proposed blind multiuser detector is designed with imprecise knowledge of the received signature waveform of the desired user. In [15] a blind adaptive multiuser detector based on Kalman filtering in both a stationary and a slowly time-varying environment is proposed. The author showed that the steady-state excess output energy of the Kalman filtering algorithm is identically zero for a stationary environment. Also, Verdu presented an overview of the adaptive tentative-decision based detectors in [13]. Verdu mentioned that the linear MMSE has the features of the decorrelating detector, except that it requires knowledge of the received amplitudes. On the other hand, the tentative decision based multiuser detector is the simplest idea for successive cancellation, but the disadvantage is that it requires extremely accurate estimation of the received amplitudes [12, 13]. Meanwhile, Verdu's work has provided exceptional important reference and guidance for the implementation of the following work.

The goal of this paper is to introduce a blind multiuser detector that adaptively recovers the signals from multiple users. In this context, the blind (or non-data aided) multiuser detector means *it requires no training data sequence, but only the knowledge of the desired user signature sequence and its timing* [9]. The proposed blind multiuser detector employs iterative an independent component analysis (ICA) algorithm at the outputs of a bank of matched filters. The main motivation of employing blind multiuser detectors in CDMA is to recover the original users' sequences from the received signals that are corrupted by multiple access interference (MAI), without the help of training sequences and a priori knowledge of the channel.

The rest of this paper is organized as follows. Section 2 gives a description of the blind multiuser detector model. Section 3 discusses the proposed ICA algorithm. A performance analysis and system capacity discussion is given in Section 4 and concluding remarks are given in Section 5.

2. Blind multiuser detector

2.1. Channel model

In DS-CDMA, each user spreads its information signal in frequency by direct sequence modulation before transmission via the common channel (Fig. 1).

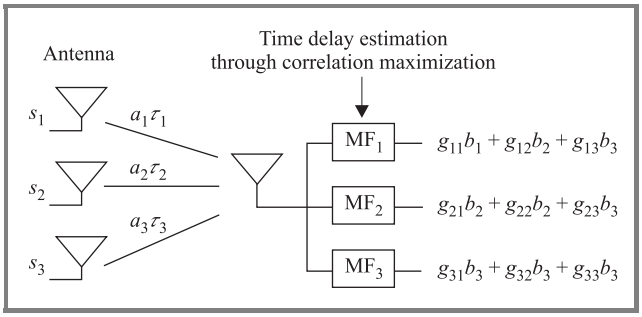


Fig. 1. *K* = 3-users detector for multiple access Gaussian channel.

We consider the K-user binary phase shift keying (BPSK) asynchronous DS-CDMA white Gaussian model as given in Eq. (1):

$$r(t) = \sum_{i=-J}^{J} \sum_{k=1}^{K} A_k b_k(i) s_k(t - iT - \tau_k) + \sigma n(t), \quad (1)$$

where:

- $2J+1$ symbols are sent by each of the K users;
- the kth signature waveform s_k is assumed to have unit energy ($\|s_k\| = 1$); $\tau_k \in [0, T)$ is the kth user's offset, where T is the symbol period; these signature sequences are independent of the data symbol, and have a chip rate much higher than that of the desired user information;
- A_k is the received amplitude of the kth user;
- b_k is the independent input data symbol of the kth user, $b_k \in \{-1, +1\}$;
- the kth signature waveform s_k is determined by the random pseudo-noise (PN) spreading sequence c_k and pulse shape waveform $p(t)$:

$$s_k(t) = \sum_{i=0}^{N_{PG}-1} c_k(i) p(t - iT_c), \quad (2)$$

where $s_k(t)$ is assumed to have unit energy over the symbol interval:

$$\begin{aligned} T &= N_{PG} T_c \quad \text{symbol interval,} \\ T_c &\quad \text{chip interval,} \\ N_{PG} &\quad \text{processing gain;} \end{aligned}$$

in this paper, we consider gold code spreading sequences; these signature sequences are independent of the data symbols and have a chip rate much higher than the symbol rate;

- the additive white Gaussian noise $n(t)$ is stationary and memoryless with unit power spectral density;
- σ^2 is the variance of noise.

We assume the users transmit completely asynchronously. In this context, when there are timing errors, each user's code experiences a random delay during the transmission and the received signal is no longer aligned with the locally generated codes [4].

For simplicity, we consider only one symbol interval. The representation for the signal during one symbol interval is written in vector form as

$$r(t) = \sum_{k=1}^{K} A_k b_k(i) s_k(t - \tau_k) + \sigma n(t). \quad (3)$$

At the receiver, the signal in Eq. (1) is chip-matched filtered and sampled at the bit rate $(1/T_b)$. The chip-matched filtered signal can be represented as

$$x_m(t) = \frac{1}{T} \int_0^T r(t) s_m(t - \tau_m + \Delta\tau_m) dt, \quad (4)$$
$$m = 1, \ldots, K,$$

where we assume a correlation maximization (or similar) operation is performed to approximately time-align the mth matched filter to the time delay τ_m of the mth user signal.

Following the sampling operation, we have:

$$x_m(i) \;=\; \text{sampled}[x_m(t)] = \sum_{k=1}^{K} g_{mk} b_k(i) + \sigma_m n(i). \quad (5)$$

The set of match-filtered signals can be represented as

$$\mathbf{x}(i) = \mathbf{G}\mathbf{b}(i) + \sigma\mathbf{n}(i), \quad (6)$$

where $\mathbf{G}$ is the matrix $\{g_{mk}\}$, m = 1, …, K, k = 1, …, K, $\mathbf{b}(i) = [b_1(i), b_2(i), \ldots, b_k(i)]^T$ and $\mathbf{n}(i)$ is a (K x 1) vector of noise samples.

2.2. Source independence

In the CDMA receiver, both code timing and channel estimation are often prerequisite tasks. Detection of the desired user's symbols in the CDMA system is far more complicated than in the simpler time division multiple access (TDMA) and frequency division multiple access (FDMA) systems used previously in mobile communications. Our main goal is to estimate and recover the original transmitted symbols. Several techniques are available

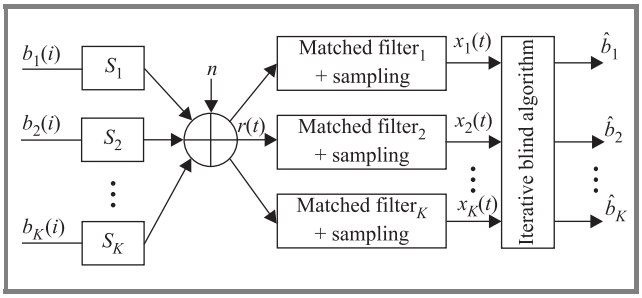


Fig. 2. K-user detection model.

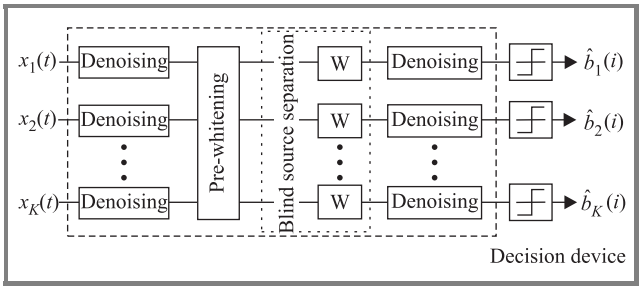


Fig. 3. The proposed blind receiver consists of PCA pre-whitening, ICA-BSS and wavelet denoising stages.

to estimate the desired user's symbols. In general, the matched filter (correlator) is the simplest estimator, but it performs well only if different users' chip sequences are orthogonal or the users have equal powers [2].

Recently, there have been attempts to apply blind and semi-blind signal processing models and algorithms in a wide variety of digital communications applications, for example multi access communications systems, multi sensor sonar and radar systems. Several good algorithms are also available for solving the basic linear and nonlinear ICA problem [1, 3, 5, 7, 10].

We propose to apply independent component analysis to design a new blind CDMA receiver. The main reason for using ICA in the CDMA receiver is because each path and user symbol sequence is typically independent of each other. The proposed multiuser detection algorithm is applied at the receiver after the wavelet denoising [8] (Figs. 2 and 3).

3. Proposed multiuser detection algorithm

The proposed algorithm is generalized from Amari's natural gradient algorithm [11]. This algorithm involves minimization of a multivariate cost function according to the stochastic gradient descent algorithm, as discussed later. The proposed algorithm, includes a pre-processing stage involving principal component analysis (PCA) (see [2, chap. 6, pp. 125–144] and [3]) of the measured sensor signals. Pre-processing is employed to pre-whiten the received signal vector, as discussed below.

3.1. Principle component analysis

Whitening of the received data $\mathbf{x}(i)$ is a common pre-processing task in ICA. In particular, a pre-whitening procedure is used mainly to decorrelate the sensor signals before separation. This makes the subsequent separation task easier, the separating matrix is then constrained to be orthogonal. There is no explicit assumption on the probability density of the vectors made in PCA [2, chap. 6, pp. 125–144], as long as the first and second order statistics are known or can be estimated from the mixture. The pre-whitened signal vector is given by

$$\mathbf{u}(i) = \boldsymbol{D}^{-1/2}\mathbf{E}^T\mathbf{x}(i)\,, \tag{7}$$

where $\mathbf{u}=[u_1,\ldots,u_K]^T$, $\mathbf{E}=(e_1,\ldots,e_K)$ is the matrix whose columns are the unit-norm eigenvectors of the covariance matrix $C_x = E\{\ \mathbf{x}(i)\ \mathbf{x}(i)^T\}$ and $\boldsymbol{D} = \mathrm{diag}(d_1,\ldots,d_K)$ is the diagonal matrix of the eigenvalues of C_x.

3.2. Proposed ICA algorithm

We now discuss the proposed ICA algorithm to unmix the source signals in the presence of noise. In the multiuser channel, $\mathbf{y}(i) = \mathbf{W}(i)\mathbf{u}(i)$, where $\mathbf{u} = [u_1, \ldots, u_K]^T$. The output components become $\mathbf{y} = g(\mathbf{u}(i))$, where the $g(\mathbf{u}(i))$ is an invertible nonlinearity. Bell and Sejnowski have shown [3] that by maximizing the join entropy of $H(\mathbf{y})$ for the neural process output can approximately minimize the mutual information among the output components $\mathbf{y}$. In this case, maximizing the joint entropy $H(y_1,\ y_2)$ of $K = 2$ output symbols, y_1 and y_2, consists of maximizing the individual entropy of each output while minimizing the mutual information $\Im(y_1, y_2)$ shared between these two output symbols [3]. The mutual information $\Im(\mathbf{y})$ between K output symbols can be deduced via Kullback-Leibler divergence:

$$\begin{aligned}\Im(\mathbf{y}) &= -H(\mathbf{y}) + \sum_{k=1}^{K} H_k(y_k)\\ &= \int_{-\infty}^{\infty} p(\mathbf{y})\log p(\mathbf{y})d\mathbf{y} - \sum_{k=1}^{K}\int_{-\infty}^{\infty} p(\mathbf{y})\log p_k(y_k)d\mathbf{y}\\ &= \int_{-\infty}^{\infty} p(\mathbf{y})\log\frac{p(\mathbf{y})}{\prod\limits_{k=1}^{K} p_k(y_k)}d\mathbf{y}\,,\end{aligned} \tag{8}$$

when the mutual information $\Im(\mathbf{y})$ is equal to zero, these K variables are statistically independent.

Then, the above mentioned differential entropy H of a random vector y_i with density $p(y_i)$ can be rewritten as

$$H(\mathbf{y}) = H(y_1)+,\ldots,+H(y_k) - \Im(\mathbf{y})\,, \tag{9}$$

where $H(y_1) = -E\Big\{\log\ \frac{p(u_1)}{|\frac{\partial y_1}{\partial u_1}|}\Big\}$,

$$\begin{aligned}H(\mathbf{y}) &= -\sum_{k=1}^{K} E\Big\{\log\frac{p(u_k)}{|\frac{\partial y_k}{\partial u_k}|}\Big\} - \Im(\mathbf{y})\\ &= -E\Big\{\log\frac{p(u_1)}{|\frac{\partial y_1}{\partial u_1}|}\Big\} + \ldots - E\Big\{\log\frac{p(u_k)}{|\frac{\partial y_k}{\partial u_k}|}\Big\} - \Im(\mathbf{y}).\end{aligned} \tag{10}$$

The goal is to learn the elements of the linear unmixing matrix $\mathbf{W}$ and the set of parameters for the nonlinearities $g(u_k(i))$. This algorithm is used to update the unmixing matrix $\mathbf{W}$. In detail, $\mathbf{W}$ is an estimate of the unknown mixing matrix of $\mathbf{u}(i)$. Using a gradient ascent algorithm, we consider the derivative of the entropy function with respect to $\mathbf{W}$ and the parameters of the nonlinearity is:

$$\begin{aligned}\frac{\partial}{\partial\mathbf{W}}(\Im(\mathbf{y})) &= -\frac{\partial H(\mathbf{y})}{\partial\mathbf{W}} - \frac{\partial}{\partial\mathbf{W}}\sum_{k=1}^{K} E\Big\{\log\frac{p(u_k)}{|\frac{\partial y_k}{\partial u_k}|}\Big\}\\ &= -(\mathbf{W}^T)^{-1} - \left(\frac{\frac{\partial p(\mathbf{u})}{\partial\mathbf{u}}}{p(\mathbf{u})}\right)\mathbf{u}^T\,.\end{aligned} \tag{11}$$

Following the work of [3, 10], we employ the following learning rule for $\mathbf{W}$

$$\Delta\mathbf{W}(\mathsf{p}) = -\alpha\frac{\partial\Im(\mathbf{y})}{\partial\mathbf{W}}\mathbf{W}^T\mathbf{W}\,, \tag{12}$$

where p is the iteration index and α the learning rate (refer to Appendix).

After initializing the weight matrix $\mathbf{W}$ and choosing α (sufficiently small value, e.g., 0.0001), the weights are iteratively updated according to the learning rule. In our observation, the learning process usually depends on the activities of the weights $\mathbf{W}$, the learning rate α, the input and output values of the mixture:

$$\mathbf{W}(\mathsf{p}+1) = \mathbf{W}(\mathsf{p}) + \alpha(\mathbf{I} - g(\mathbf{y})\mathbf{y}^T + \mathbf{y}(g(\mathbf{y}))^T)\mathbf{W}(\mathsf{p}), \quad (13)$$

where p is the iteration index.

The proposed algorithm for complex signals performs as follows:

1. Chip-matched filtered signals, wavelet denoising.
2. PCA pre-whitening the signals.
3. Select an initial separating matrix $\mathbf{W}_0$ and learning rate α.
4. Determine and estimate the initial, $\mathbf{y} = \mathbf{W}_0\mathbf{u}$.
5. Update the separating matrix by $\mathbf{W}_{\mathsf{p}+1} \longleftarrow \mathbf{W}_{\mathsf{p}} + \alpha(\mathbf{I} - g(\mathbf{y})\mathbf{y}^T + \mathbf{y}(g(\mathbf{y}))^T)\mathbf{W}_{\mathsf{p}}$, where $\mathbf{I}$ is the identity matrix.
6. Decorrelate and normalize $\mathbf{W}_{\mathsf{p}+1}$.
7. If $|(\mathbf{W}_{\mathsf{p}+1})^T\mathbf{W}_{\mathsf{p}}|$ is not close enough to 1, then p = p+1, and go back to Step 5. Else, output the vector $\mathbf{W}_{\mathsf{p}}$.
8. Wavelet denoising.
9. Output detector, sgn $(\mathbf{y})$.

3.3. Error measure

The performance during the learning process was monitored by an error measure based on:

$$\mathbf{PI} = \frac{1}{K^2}\left(\sum_{i=1}^{K}\left(\sum_{j=1}^{K}\frac{|PD_{ij}|}{\max_k |PD_{ik}|} - 1\right) + \sum_{j=1}^{K}\left(\sum_{i=1}^{K}\frac{|PD_{ij}|}{\max_k |PD_{kj}|} - 1\right)\right), \quad (14)$$

where PD_{ij} is the (i,j)th element of $\mathbf{PD} = \mathbf{WG}$, $\mathbf{G}$ is the unknown mixing matrix and K is the number of users. **PD** is close to the permutation of the scaled identity matrix when the sources are separated. This corresponds to **PI** = 0.

4. Numerical experiments

The proposed blind multiuser detector has been examined in various experimental situations. Several results are presented to compare the proposed blind multiuser detector with correlating detector, matched filter bank and blind MMSE detectors [6]. For each run, these 4 detectors are applied at the same time. The following experiments are mainly to demonstrate the performance of the multiuser detectors with varying signal-to-noise ratio (SNR) levels and power levels. These experiments are also to demonstrate the performance of the proposed method in multiuser interference (MAI).

We consider using a simulated DS-CDMA data with additive white Gaussian noise (AWGN) channel and two antenna elements in the reception with a half a carrier wavelength spacing, unless mentioned otherwise. All CDMA signals are generated with BPSK data modulation and gold codes of length 61 are used as the spreading codes. The length of the block was 40 non-coherent BPSK symbols, during which the channel was fixed. The number of signals distribution, and the path delays were randomly chosen. Matched-filter bank, decorrelating detector and blind MMSE detector receivers were used as reference methods.

We first present the performance of the proposed algorithm by presenting the numerical values of the bit error rate (BER) as a function of SNR in Fig. 4. The system consists of K = 2 users and both users are assigned with equal

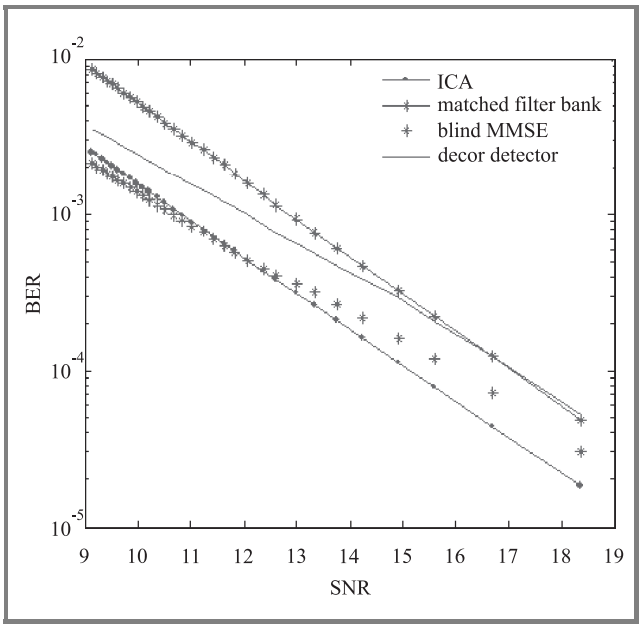


Fig. 4. Bit error rate as a function of SNR for decorrelating detector, matched filter bank, blind MMSE and ICA detectors.

power. The proposed ICA detector based method shows the lowest BER compared to blind MMSE method, matched filter bank and decorrelating detector especially at lower SNR. The convergence of the gradient approach took place in 10–15 iterations in this case. The ICA detector displays better performance compared to the matched filter bank, and decorrelating detectors. However, the performances of the proposed ICA and adaptive blind MMSE detector are very close to each other. The adaptive blind MMSE detector slightly outperforms the ICA detector from 9 dB to 11 dB. Then, ICA detector shows better performance after 12 dB onwards. The margin of improvement becomes larger with increased SNR.

We then implement the multiple access interference channels to demonstrate the ability of the mentioned detectors dealing with large number of users within the same channel as shown in Fig. 5. ICA analysis proved to be better per-

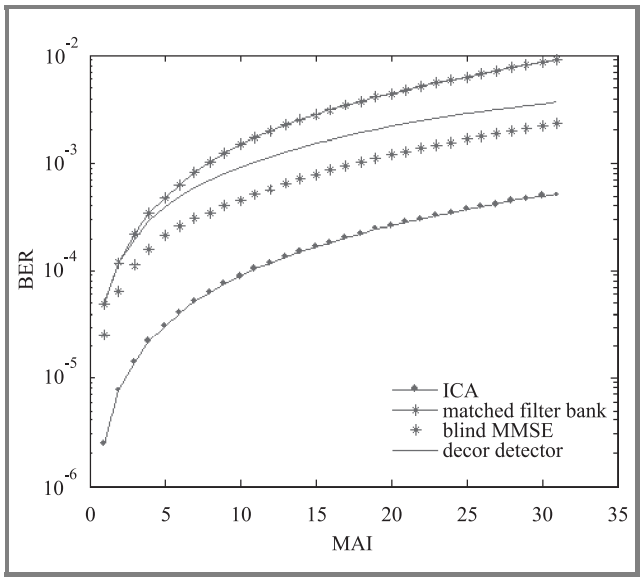


Fig. 5. Bit error rate plots versus K users in MAI channel using ICA, blind MMSE, matched filter bank and decorrelating detectors.

forming technique; it is then followed by the blind MMSE detector, matched filter bank and the decorrelating detectors. We observed that the matched filter and decorrelating detector are not able to work in multiple access interference environment (which industries require BER $\leq 10^{-3}$), which the figure shown high BER with increasing MAI.

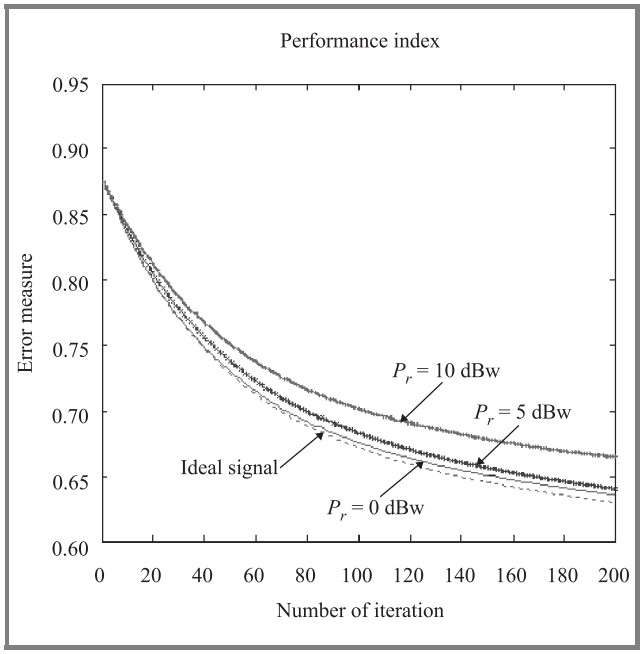


Fig. 6. Error measure for various power levels of multi access interference using the ICA multiuser detector.

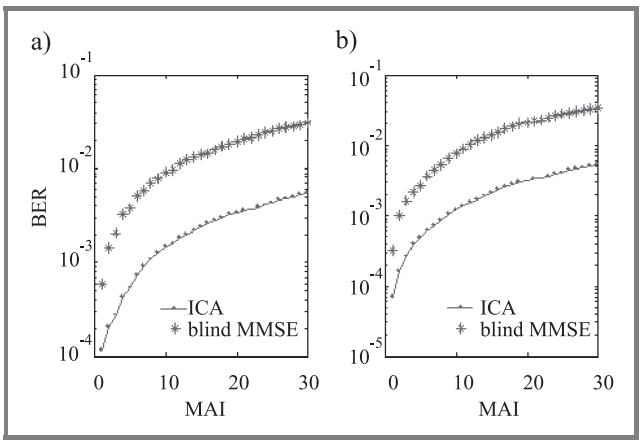


Fig. 7. Bit error rate versus MAI for SNR = 8 dB for various levels of signal power: (a) 15 dBw; (b) 5 dBw.

The error measure due to MAI is illustrated graphically in Figs. 6 and 7 for CDMA system. In this experiment, power level of the interfering signals (P_r) are 0 dBw, 5 dBw and 10 dBw respectively with SNR of 10 dB and the desired signal at 0 dBw. For comparison purposes, we include an "ideal" case, coresponding to no MAI and an SNR of 16 dB. Clearly, the ICA detector shows better performance, in which the error measure for the intefereing signal cases of 0 dBw, 5 dBw and 10 dBw is 0.635, 0.64 and 0.665, respectively. This is due to the proposed detector's denoising nature dealing with noisy channels.

5. Discussion

We have proposed a new methodology for the design of asynchronous multiuser CDMA system. The design is based on blind source separation in the DS-CDMA communication system by means of independent component analysis. The blind CDMA detectors are interference cancellers with ICA analysis to decrease the cross correlation between the users by employing multiple matched filters at the receiver. Since the signature sequences are known a priori, the accuracy obtained when estimating these parameters becomes high. The experimental results show that the proposed blind ICA multiuser detectors perform better in multiaccess interference than the blind MMSE, matched filter bank and decorrelating detectors. In particular, the main reasons for considering ICA as an additional tuning element in the next generation CDMA system are the following:

- ICA is worth considered as an additional element, attached to some existing receiver structure to perform the task of user identification.

- Since the original CDMA detection and estimation methods do not exploit the powerful but realistic independence assumption [2], ICA (with the independence of the source signals is utilized) would offer an

additional interference suppression capability to the CDMA detection [14].

- Since the receiver has some prior information on the communication system; typically at least the spreading code of the desired user is known, ICA can easily function in CDMA receiver.
- ICA is particularly to unmix the mixed signals to recover the original source signals. Therefore, it is able to mitigate additional multiple access interference to enhance the performance of detectors.

6. Conclusion

In this paper, we have designed a blind ICA multiuser detector based on the ICA algorithm. Several simulation results show that the blind multiuser detector provides a significant performance improvement compared to other multiuser detectors. We conclude that blind ICA detector is suitable for the next generation wireless CDMA communication system.

Appendix

The update for the mixing matrix $\mathbf{W}$ is determined via the gradient of the mutual information with respect to the elements of $\mathbf{W}$. Essentially, $\mathbf{W}$ is an estimate of $\mathbf{G}^{-1}$, where $\mathbf{G}$ is the unknown mixing matrix of $\mathbf{u}(i)$.
The updated elements of $\mathbf{W}$ in the natural gradient based optimization algorithm are given by

$$\mathbf{W}_{\mathsf{update}} = \mathbf{W} + \triangle\mathbf{W} = \mathbf{W} - \frac{\partial \Im(y_1,\ldots,y_K)}{\partial \mathbf{W}}\mathbf{W}^T\mathbf{W}, \quad (15)$$

where $\Im(y_1,\ldots,y_K)$ is the mutual information between the output signals where:

$$\Im(y_1,...,y_K) = E\{\log\ p(\mathbf{u})\} - \log(\det\mathbf{W}) - \sum_{k=1}^{K} E\{\log p_k(y_k)\}. \quad (16)$$

When the mutual information $\Im(\mathbf{y})$ is equal to zero, these variables $y_1,\ldots,y_K$ are statistically independent. The gradient of $\Im(y_1,\ldots,y_K)$ with respect to $\mathbf{W}$ can be expressed as

$$\frac{\partial \Im(y_1,\ldots,y_K)}{\partial \mathbf{W}} = \frac{\partial E\{\log(p(\mathbf{u}))\}}{\partial \mathbf{W}} - \frac{\partial\{\log(\det\mathbf{W})\}}{\partial \mathbf{W}} - \frac{\partial\sum_{k=1}^{K} E\{\log p(y_k)\}}{\partial \mathbf{W}}$$

$$= -\frac{\partial\{\log(\det\mathbf{W})\}}{\partial \mathbf{W}} - \sum_{k=1}^{K}\frac{\partial E\{\log p(y_k)\}}{\partial \mathbf{W}} \quad (17)$$

since the first term, $E\{\log\ p(\mathbf{u})\}$ does not involve $\mathbf{W}$. We will analyze the two remaining terms separately. In the case of the first term, we have:

$$\frac{\partial\{\log(\det\mathbf{W})\}}{\partial \mathbf{W}} = \frac{1}{\det\mathbf{W}}\frac{\partial \det\mathbf{W}}{\partial \mathbf{W}} = \frac{1}{\det\mathbf{W}}(adj(\mathbf{W}))^T = (\mathbf{W}^{-1})^T. \quad (18)$$

From the second term in Eq. (19), we have incorporated the density function $p_k(y_k)$:

$$\sum_{k=1}^{K}\frac{\partial E\{\log(p(y_k))\}}{\partial \mathbf{W}}$$

$$= \sum_{k=1}^{K} E\left\{\frac{1}{p_k(y_k)}\frac{\partial p_k(y_k)}{\partial (y_k)}\frac{\partial y_k}{\partial \mathbf{W}}\right\}$$

$$= E\begin{pmatrix} \frac{1}{p_1(y_1)}\frac{\partial p_1(y_1)}{\partial (y_1)}u_1 & \cdots & \frac{1}{p_1(y_1)}\frac{\partial p_1(y_1)}{\partial (y_1)}u_K \\ \vdots & & \vdots \\ \frac{1}{p_K(y_K)}\frac{\partial p_K(y_K)}{\partial (y_K)}u_1 & \cdots & \frac{1}{p_K(y_K)}\frac{\partial p_K(y_K)}{\partial (y_K)}u_K \end{pmatrix}$$

$$= E\left\{\frac{1}{p(\mathbf{y})}\frac{\partial p(\mathbf{y})}{\partial (\mathbf{y})}\mathbf{u}^T\right\}, \quad (19)$$

where by $p(\mathbf{y})$ we mean $(p_1(y_1),\ldots,p_K(y_K))$.

The natural gradient of $\Im(y_1,\ldots,y_K)$ is given in Eq. (20). The minimum mutual information algorithm for ICA will repeatedly perform an update of the matrix $\mathbf{W}$:

$$\Delta\mathbf{W}_{\mathsf{p}} = \mathbf{W}_{\mathsf{p+1}} - \mathbf{W}_{\mathsf{p}} = -\frac{\partial \Im(\mathbf{y})}{\partial \mathbf{W}}\mathbf{W}^T\mathbf{W} = [\mathbf{I} - g(\mathbf{y})\mathbf{y}^T]\mathbf{W}, \quad (20)$$

where $\mathbf{I}$ is the identity matrix and

$$g(\mathbf{y}) = \frac{1}{p(\mathbf{y})}\frac{\partial p(\mathbf{y})}{\partial \mathbf{y}} = \frac{\partial}{\partial \mathbf{y}}\log(p(\mathbf{y})). \quad (21)$$

The multiplication with the natural gradient not only preserves the direction of the gradient but also speeds up the convergence process.
The formulation of Eq. (20) requires that each $\{g_k(y_k)\}_{k=1}^{K}$ is a nonlinear function corresponding to a symmetric density. Ideally the nonlinear function $g_k(y_k)$ approximates

the probability density function of y_k. The nonlinear function applied in this work is as follows:

$$g_k(y_k) = \mathrm{abs}(y_k^{0.9}(i)) \cdot \mathrm{sgn}(y_k(i)) \,. \tag{22}$$

After initializing the weight matrix $\mathbf{W}_0$ with identity matrix, and choosing α as sufficiently small constant, e.g., 0.0001, the weights are iteratively updated according to the learning rule in Eq. (23). Indeed, the learning process usually depends on the activities of the weights $\mathbf{W}$, learning rate α, nonlinearity g($\mathbf{y}$), input and output values of the mixture. The Eq. (20) is extended as

$$\mathbf{W}_{\mathsf{p}+1} = \mathbf{W}_{\mathsf{p}} + \alpha\big(\mathbf{I} - g(\mathbf{y})\mathbf{y}^T + \mathbf{y}(g(\mathbf{y}))^T\big)\mathbf{W}_{\mathsf{p}} \,, \tag{23}$$

where p is the iteration index, $\mathbf{I}$ is the identity matrix, and the estimated output $\mathbf{y}_{\mathsf{p}}(i) = \mathbf{W}_{\mathsf{p}}\mathbf{u}(i)$.

References

[1] A. Hyvarinen and E. Oja, "Independent component analysis: a tutorial", Tech. Rep., Helsinki University of Technology, Apr. 1999.

[2] A. Hyvarinen, J. Karhunen, and E. Oja, *Independent Component Analysis*. Wiley, 2001.

[3] A. J. Bell and T. J. Sejnowski, "An information maximization approach to blind separation and blind deconvolution", *Neur. Computat.*, vol. 7, pp. 1129–1159, 1995.

[4] H. Delic and A. Hocann, "Robust detection in DS-CDMA", *IEEE Trans. Veh. Technol.*, vol. 51, pp. 155–170, 2002.

[5] H. Mathis, "Nonlinear functions for blind separation and equalization", Ph.D. thesis, Hartung-Gorre, Konstanz, Nov. 2001.

[6] M. Honig, U. Madhow, and S. Verdu, "Blind adaptive multiuser detection", *IEEE Trans. Inform. Theory*, vol. 41, pp. 944–960, 1995.

[7] P. Comon, "Independent component analysis, a new concept?", *Higher-Order Stat.*, vol. 36, no. 3, pp. 287–314, 1994.

[8] R. R. Coifman and D. L. Donoho, "Translation-invariant denoising", Tech. Rep., Yale University and Stanford University, 1995.

[9] D. Samardzija, N. Mandayam, and I. Seskar, "Blind successive interference cancellation for DS-CDMA systems", *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 276–290, 2002.

[10] S. Amari, "Natural gradient works efficiently in learning", *Neur. Computat.*, vol. 10, pp. 251–276, 1998.

[11] S. Amari, "Stability analysis of adaptive blind source separation", Tech. Rep., Brain Information Processing Group, 1997.

[12] S. Verdu, "Adaptive multiuser detection", in *IEEE Third Int. Symp. Spr. Spectr. Tech. Appl. ISSSTA'94*, Oulu, Finland, 1994, vol. 1, pp. 43–50.

[13] S. Verdu, *Multiuser Detection*, 2nd ed. Cambridge: Cambridge University Press, 2001, chap. 2.

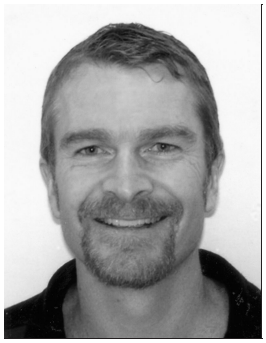
[14] T. Ristaniemi and J. Joutsensalo, "Advanced ICA-based receivers for blocking fading DS-CDMA channels", *Sig. Proces.*, vol. 82, pp. 417–431, 2002.

[15] X. D. Zhang and W. Wei, "Blind adaptive multiuser detection based on Kalman filtering", *IEEE Trans. Sig. Proces.*, vol. 50, no. 1, pp. 87–95, 2002.

Wai Yie Leong received the B.Sc. degree in electrical engineering and the Ph.D. degree in electrical engineering from The University of Queensland, Australia, in 2002 and 2006, respectively. In 2005, she joined the School of Electronics and Electrical Engineering, Imperial College London, United Kingdom, where she is currently working as a post-doctoral research fellow. Her research interests include blind source separation, blind extraction, mobile communication systems, smart antennas and biomedical engineering. She was a recipient of the Queensland Smart State SmartWomen (Australia) in 2005.

School of Information Technology
and Electrical Engineering
The University of Queensland
Brisbane QLD 4072, Australia

e-mail: w.leong@imperial.ac.uk
School of Electronics and Electrical Engineering
Imperial College London
South Kensington, SW7 2BT, United Kingdom



John Homer received the B.Sc. degree in physics from the University of Newcastle, Australia, in 1985 and the Ph.D. degree in systems engineering from the Australian National University, Canberra, Australia, in 1995. Between his B.Sc. and Ph.D. studies he held a position of Research Engineer at Comalco Research Centre in Melbourne, Australia. Following his Ph.D. studies he has held research positions with the University of Queensland, Veritas DGC Pty Ltd and Katholieke Universiteit Leuven, Belgium. He is currently a Senior Lecturer at the University of Queensland within the School of Information Technology and Electrical Engineering. His research interestes include signal and image processing, particularly in the application areas of telecommunications, audio and radar. He is currently an Associate Editor of the "Journal of Applied Signal Processing".

e-mail: homerj@itee.uq.edu.au
School of Information Technology
and Electrical Engineering
The University of Queensland
Brisbane QLD 4072, Australia

Paper

A highly accurate DFT-based parameter estimator for complex exponentials

Jeffrey Tsui and Sam Reisenfeld

Abstract— A highly accurate DFT-based complex exponential parameter estimation algorithm is presented in this paper. It will be shown that for large number of samples and high signal to noise ratio (SNR), the phase estimation error variance performance is only 0.0475 dB above the Cramer-Rao lower bound (CRLB) for phase estimation with unknown frequency and phase. The amplitude estimation error variance performance was found to lay on the CRLB for amplitude estimation. Exact phase and amplitude estimation can be achieved in the noiseless case with this algorithm. The algorithm has low implementation computational complexity and is suitable for numerous real time digital signal processing applications.

Keywords— frequency estimation, phase estimation, amplitude estimation, DFT-based parameter estimation, spectral estimation, digital signal processing algorithm, complex exponential parameter estimation.

1. Introduction

Frequency, phase and amplitude estimation of a complex exponential is classical problem in statistical signal processing. The precision of the phase and amplitude estimate is directly related to the accuracy of the frequency estimate. There are two major classes of complex exponential frequency estimation algorithm in the existing literature. The first class is the classical discrete Fourier transform (DFT) and phase averager based frequency estimation algorithms such as [3] and [4]. This class of estimation algorithm is very computationally efficient, however they suffer from poor error performance at low signal to noise ratio (SNR). The second class is the parametric frequency estimation algorithms such as the very popular MUSIC and ESPRIT algorithms [5, 6]. This class of estimation algorithm has very good error performance across a wider range of SNR, however, they are very computationally intensive and not suitable for real-time application. Obviously, it would be ideal if there exists a complex exponential parameter estimator that is both computationally efficient and has good performance at low SNR.

In 2003, Reisenfeld and Aboutanios [2] discovered a frequency estimator that can precisely estimating the frequency of a complex exponential in an iterative manner by applying contraction mapping method on two modified DFT coefficients. In a subsequence publication in 2004, Reisenfeld [1] further enhanced the previous published algorithm by improving the convergence property of the estimator. It can be shown that this particular frequency estimator can yield a frequency estimate that is 0.0633 dB of the Cramer-Rao lover band (CRLB) with approximately $N\log_2 N + 4N$ complex multiplications, where N is the number of samples used representing the signal.

In this paper, it will be shown that combining the said frequency estimator with maximum likelihood (ML) phase and amplitude estimators yields a highly accurate parameter estimator for complex exponentials. In the noiseless case, it is possible to obtain the exact phase and amplitude estimates with this estimator. In additive white Gaussian noise (AWGN) channel, the said estimates approach very close the their respective CRLB at relative high SNR. The relationship between the number of samples, N, and the operating point of the parameter estimator in terms of SNR will be given. It will also be shown that it is possible to use the said relationship to further optimise the computation complexity of the estimator.

The rest of the paper will be organised as follows: Section 2 introduces the proposed DFT-based parameter estimator, Section 3 will provide the performance analysis of the proposed parameter estimator. Section 4 will describe further enhancements that can be made to the original frequency estimator in [1] to reduce its computation complexity. Section 5 contains the simulated results of the performance of the proposed algorithm and this will be followed by the conclusion.

2. The DFT-based parameter estimator

The proposed DFT-based parameter estimator involves a two stage process. First, the frequency of the received carrier is estimated by the frequency estimator as described in [1]. The frequency estimate obtained is then used to eliminate the frequency component of the carrier, leaving only the phase and amplitude component to be estimated by the ML phase and amplitude estimator.

2.1. The DFT-based complex exponential frequency estimator

Consider a complex exponential, $r[n]$, with amplitude, A_c, frequency, $f_c \in [0, f_s)$, and phase $\theta_c \in [0, 2\pi)$. Mathematically, $r[n]$ can be represented as

$$r[n] = A_c e^{j(2\pi f_c n T_s + \theta_c)} + \eta[n], \tag{1}$$

where $n = 0, 1, 2, ..., N-1$, $T_s = 1/f_s$ is the sampling period, and $\eta[n]$ is a sequence of independent complex Gaussian variables with mean of zero and variance σ^2.

In noiseless condition, the magnitude spectra the DFT of Eq. (1) will have even symmetry about its frequency. The recursive algorithm as described in [1] exploits this condition by employing a discriminate that works on a contraction principle in minimizing the difference in the magnitude of two modified DFT coefficients which are plus and minus half a DFT bin away from an estimated frequency. Due to the even symmetric nature of the magnitude spectra, the difference in the magnitude of the two modified DFT coefficients will eventually reduced to zero in the noiseless case as the estimated frequency approaches the true frequency with the increasing number of recursions of the algorithm. The frequency can then be estimated as the mean of the frequencies of the modified DFT coefficients at which difference in their magnitude equals to zero.
Summarizing the DFT-based frequency estimator in [1]:

1. Perform a coarse frequency estimate such as the one described in Rife and Boorstyn [3], in which $\{r[n]\}_0^{N-1}$ is the input to a N point complex DFT and a peak search is done on the magnitudes of the DFT output coefficients, to obtain the initial frequency estimate, $\hat{f}_0$. This estimate is obtained by, $\hat{f}_0 = k_{\max} f_s / N$, where $k_{\max}$ is the index of the maximum magnitude DFT output coefficient.

2. Calculate the modified DFT coefficients α_m and β_m defined by

$$\alpha_m = \sum_{n=0}^{N-1} r[n]\, \mathrm{e}^{-\mathrm{j}2\pi n\left(\hat{f}_m T_s - \frac{1}{2N}\right)}, \tag{2}$$

$$\beta_m = \sum_{n=0}^{N-1} r[n]\, \mathrm{e}^{-\mathrm{j}2\pi n\left(\hat{f}_m T_s + \frac{1}{2N}\right)}. \tag{3}$$

3. Calculate the discriminate D_m defined as

$$D_m = \frac{|\beta_m| - |\alpha_m|}{|\beta_m| + |\alpha_m|}. \tag{4}$$

4. Calculate the new adjusted frequency with the formula:

$$\hat{f}_{m+1} = \hat{f}_m + \frac{1}{\pi} \tan^{-1}\left[D_m \tan\left(\frac{\pi}{2N}\right)\right] f_s. \tag{5}$$

5. Perform Steps 2–4 recursively for $m = 1, 2, 3, \ldots, M-1$.

2.2. Combining the frequency estimator with ML phase and amplitude estimator

Using the frequency estimate $\hat{f}_m$ obtained from the frequency estimator described above, it is possible to eliminate the frequency component of $r[n]$ by multiplying it with the conjugate of the complex exponential with a frequency of $\hat{f}_m$. Denoting $r_{A,\theta}[n]$ as the result of the multiplication we have

$$\begin{aligned} r_{A,\theta}[n] &= \left(A\mathrm{e}^{\mathrm{j}(2\pi f_c n T_s + \theta_c)} + \eta[n]\right) \cdot \mathrm{e}^{-\mathrm{j}2\pi \hat{f}_m n T_s} \\ &= A\mathrm{e}^{\mathrm{j}(2\pi \varepsilon n T_s + \theta_c)} + \eta[n], \end{aligned} \tag{6}$$

where $\varepsilon = f_c - \hat{f}_m$.
It was shown in [7] that the ML phase estimate of a complex exponential is obtained by taking its arctangent. Taking the arctangent of $\sum_{n=0}^{N-1} r_{A,\theta}[n]$ yields

$$\begin{aligned} \hat{\theta}_{c,\hat{f}_m} &= \tan^{-1}\left(\frac{\mathrm{Im}\left[\sum_{n=0}^{N-1}\left(A\mathrm{e}^{\mathrm{j}(2\pi \varepsilon n T_s + \theta_c)} + \eta[n]\right)\right]}{\mathrm{Re}\left[\sum_{n=0}^{N-1}\left(A\mathrm{e}^{\mathrm{j}(2\pi \varepsilon n T_s + \theta_c)} + \eta[n]\right)\right]}\right) \\ &= \tan^{-1}\left(\frac{\sum_{n=0}^{N-1} A\sin(2\pi \varepsilon n T_s + \theta_c) + \eta_s}{\sum_{n=0}^{N-1} A\cos(2\pi \varepsilon n T_s + \theta_c) + \eta_c}\right), \end{aligned} \tag{7}$$

where

$$\eta_c = \mathrm{Re}\left(\sum_{n=0}^{N-1} \eta[n]\right), \quad E[\eta_c] = 0, \quad Var[\eta_c] = \frac{N\sigma^2}{2}, \tag{8}$$

$$\eta_s = \mathrm{Im}\left(\sum_{n=0}^{N-1} \eta[n]\right), \quad E[\eta_s] = 0, \quad Var[\eta_s] = \frac{N\sigma^2}{2}, \tag{9}$$

and $\hat{\theta}_{c,f_m}$ is the phase estimate based upon the estimated frequency.
It was also shown in [7] that the ML amplitude estimate of a complex exponential is obtained by taking its absolute value. Taking the absolute value of $\sum_{n=0}^{N-1} r_{A,\theta}[n]$ yields

$$\begin{aligned} \hat{A}_{\hat{f}_m} &= \frac{1}{N}\sqrt{\mathrm{Re}\left[\sum_{n=0}^{N-1}\left(A\mathrm{e}^{\mathrm{j}(2\pi \varepsilon n T_s + \theta_c)} + \eta[n]\right)\right]^2 + \mathrm{Im}\left[\sum_{n=0}^{N-1}\left(A\mathrm{e}^{\mathrm{j}(2\pi \varepsilon n T_s + \theta_c)} + \eta[n]\right)\right]^2} \\ &= \frac{1}{N}\sqrt{\left[\sum_{n=0}^{N-1} A\cos(2\pi \varepsilon n T_s) + \eta_c\right]^2 + \left[\sum_{n=0}^{N-1} A\sin(2\pi \varepsilon n T_s) + \eta_s\right]^2}. \end{aligned} \tag{10}$$

Notice the amplitude estimation is not affected by the phase angle of the complex exponential θ_c.
From Eqs. (7) and (10), it is obvious that a highly accurate frequency estimator can assist in reducing the error and improve on the accuracy of the phase estimation. Hence the described frequency estimator is very suitable for this joint estimation of phase and amplitude due to its superior error variance performance.

3. Performance of the parameter estimator

3.1. Frequency estimator

The author in [1] has proven this algorithm only requires two iterations for the variance of the frequency estimate $\hat{f}_2$ to converge to less than or equal to 0.063 dB above the CRLB for frequency estimation.

3.2. Phase estimator

Assuming high SNR, using Taylor series expansion as described in [8] the variance of Eq. (7) was found to be

$$Var\left[\hat{\theta}_{c,\hat{f}_m}\right] = \frac{N^2(N-1)^2\sin^2\left(\frac{\pi}{2N}\right)\tan^2\left(\frac{\pi}{2N}\right)+2}{4\rho N}, \quad (11)$$

where ρ, the SNR equals to

$$\rho = \frac{A^2}{\sigma^2}. \quad (12)$$

Since this algorithm jointly estimates the frequency and phase of the observed signal, it is appropriate to compare the performance of the phase estimator to the CRLB of phase estimation with unknown frequency and phase which is given by [7]

$$CRLB_{joint}(\theta) = \frac{(2N-1)}{N\rho(N+1)}. \quad (13)$$

Therefore

$$\frac{Var\left[\hat{\theta}_{c,\hat{f}_m}\right]}{CRLB_{joint}(\theta)} = \frac{\left(N^2(N-1)^2\sin^2\left(\frac{\pi}{2N}\right)\tan^2\left(\frac{\pi}{2N}\right)+2\right)(N+1)}{4(2N-1)}. \quad (14)$$

For large ρ and large N, it can be shown,

$$\lim_{N\to\infty} 10\log_{10}\left(\frac{Var\left[\hat{\theta}_{c,\hat{f}_m}\right]}{CRLB_{joint}(\theta)}\right) = 10\log_{10}\left(\frac{\pi^4}{128}+\frac{1}{4}\right) = 0.0475 \text{ dB}. \quad (15)$$

Figure 1 shows the convergence property of $Var\left[\theta_{est,f}\right]$ to the CRLB as a function of the number of samples N. It can be seen that variance of the phase estimator deviates from the CRLB as the number of samples N increases and approaches the asymptotic limit of 0.0475 dB. This due to the convergence behavior of the frequency estimator as stated in [1] where for small N, less information is discarded for not using all the DFT coefficients hence the performance degradation is less than when N is large.

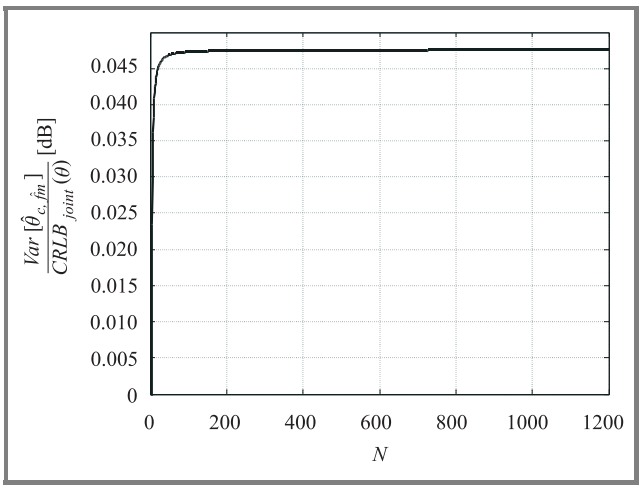


Fig. 1. $\frac{Var[\hat{\theta}_{c,\hat{f}_m}]}{CRLB_{joint}(\theta)}$ in dB as a function of number of samples, N.

3.3. Amplitude estimator

Assuming high SNR, using Taylor series expansion as described in [8] the variance of Eq. (10) was found to be

$$Var\left[\hat{A}_{\hat{f}_m}\right] = \frac{\sigma^2}{2N}, \quad (16)$$

which agrees with the CRLB derived by Rife and Boorstyn in [3].

4. Further enhancements

As describe in Subsection 2.1, the frequency estimator in [1] requires an initial frequency estimate obtained by performing a fast Fourier transform (FFT) operation on the signal samples. Since FFT requires $N\log_2 N$ complex multiplications, it is desirable to keep the number of samples N as low as possible for the initial coarse estimate. However, the CRLB for frequency estimation monotonically decreases with the increasing number of samples used for the estimation at a fixed SNR. Hence, reducing the number of samples used for the frequency estimate may not produce an estimate that will meet the required accuracy.

One way to reduce the complexity of the estimator and obtain the required accuracy is to modify the frequency estimator so that it beings the initial coarse frequency estimation with a low number of samples and dynamically increase the number of samples for each iteration of frequency estimation algorithm. The modified version of the DFT-based frequency estimator is summarised as follows:

Denoting N_i, where $i = 0,1,2,3,...,I$, as the number of samples used in the ith pass of the frequency estimation algorithm. Note that the number of samples, N_i, for each pass must satisfy the following relationship $N_0 \le N_1 \le N_2 \le ... \le N_I$ and $N_I = N$ which is the number of samples required to obtain the desire accuracy.

1. Perform a coarse frequency estimate such as the one described in Rife and Boorstyn [3], in which $\{r[n]\}_0^{N_0-1}$ is the input to a N_0 point complex DFT

and a peak search is done on the magnitudes of the DFT output coefficients, to obtain the initial frequency estimate, $\hat{f}_0$. This estimate is obtained by, $\hat{f}_0 = k_{\max} f_s / N_0$, where $k_{\max}$ is the index of the maximum magnitude DFT output coefficient.

2. Perform the ith pass of the frequency estimator which consists of the following steps:

   2.1. Recursion is started at $m = 0$.

   2.2. Set $N_i = N_0$.

   2.3. Calculate the modified DFT coefficients α_m and β_m defined by

$$\alpha_m = \sum_{n=0}^{N_i-1} r[n]\, \mathrm{e}^{-\mathrm{j}2\pi n\left(\hat{f}_m T_s - \frac{1}{2N_i}\right)}, \tag{17}$$

$$\beta_m = \sum_{n=0}^{N_i-1} r[n]\, \mathrm{e}^{-\mathrm{j}2\pi n\left(\hat{f}_m T_s + \frac{1}{2N_i}\right)}. \tag{18}$$

   2.4. Calculate the discriminate D_m defined as

$$D_m = \frac{|\beta_m| - |\alpha_m|}{|\beta_m| + |\alpha_m|}. \tag{19}$$

   2.5. Calculate the new adjusted frequency with the formula:

$$\hat{f}_{m+1} = \hat{f}_m + \frac{1}{\pi} \tan^{-1}\left[D_m \tan\left(\frac{\pi}{2N_i}\right)\right] f_s. \tag{20}$$

   2.6. Perform Steps 2.3–2.5 recursively for $m = 1, 2, 3, \ldots, M-1$.

3. Set the value of $\hat{f}_0$ to the value of $\hat{f}_m$ as found in Step 2.5. Repeat Step 2 for $N_i = N_1$, $N_i = N_2, \ldots$, $N_i = N_I$.

Choosing the value of N_i's. Thus far, the discussion has been on the reducing the number of samples to save computational complexity. However, the question of how one practically chose the values of N_i's remains. The choices of the value of the N_i's are govern by the frequency error variance of the estimate from the individual ith passes. If the frequency estimate, $\hat{f}_m$, of the ith was too far away from actual frequency, it will cause the frequency estimator converge on an incorrect frequency. In fact, in the original algorithm presented in [1], the initial frequency estimate error must be bound between the frequency that is represented by $\pm 1/2$ of a DFT bin to ensure convergence of the algorithm. Since we are increasing the number of samples, N_i, at each pass, one must ensure the frequency estimate error of the ith pass must be smaller than $\pm 1/2$ the frequency represented by a DFT bin of the next pass. This relationship can be mathematically represented as

$$\sqrt{\frac{N_i \sin^2\left(\frac{\pi}{2N_i}\right) \tan^2\left(\frac{\pi}{2N_i}\right)}{4\rho\pi^2}} \leq \frac{1}{2N_{i+1}}. \tag{21}$$

In addition to the above condition, the value of N_0, which corresponds to the length of initial FFT for the initial peak search, has an extra constraint in the form of the performance threshold at low SNR as discussed in [3]. The performance threshold has to do with the nonlinear nature of the frequency estimation problem as low SNR. A detail discussion on the relationship between performance threshold, SNR and the number of samples is out of the scope of this paper. There are a number of papers that addresses this issue and readers are recommended to look at references [9–12] for detail analysis of performance threshold. Only the findings from [9] are discussed in this paper because of the simplistic nature of the results and the ease of applying them to determine the optimum value of N_0 given it has to operate above certain SNR.

In [9], the author derived an approximate threshold indicator given by

$$E\,(N\delta^*)^2 = \frac{3}{2\rho N}, \tag{22}$$

where δ^* is the approximation of the normalised frequency error. It was found there is a relationship between the indicator quantity given in Eq. (22) and the mean square (MS) phase error given by

$$E\,(N\delta^*)^2 = \frac{3}{2\rho N} = \frac{3}{4} E\left(\tilde{\theta}\right)^2. \tag{23}$$

The author in [9] also found the MS phase error associated with the threshold is roughly $E\left(\tilde{\theta}\right)^2 = 0.0625$ rad^2. Table 1 was built using Eq. (23) at common values of N.

Table 1
SNR threshold for various values of N

N	Threshold SNR [dB]
1024	−15.05
512	−12.04
256	−9.03
128	−6.02
64	−3.01
32	0

Since these threshold values are approximations, one should allow a operating margin of at least 1.5 dB when deciding upon the value of N_0. For example, if the requirement is for the estimator to operate at −3 dB, one would choose $N_0 = 128$ over $N_0 = 64$ to guarantee proper operation at −3 dB. Compare the values in Table 1 to the relationship as stated in Eq. (21), one can conclude the performance threshold will dominate in deciding on the value of N_0.

5. Simulation results

Figures 2, 3 and 4 shows the simulated results of the error variance performance as a function of SNR for the fre-

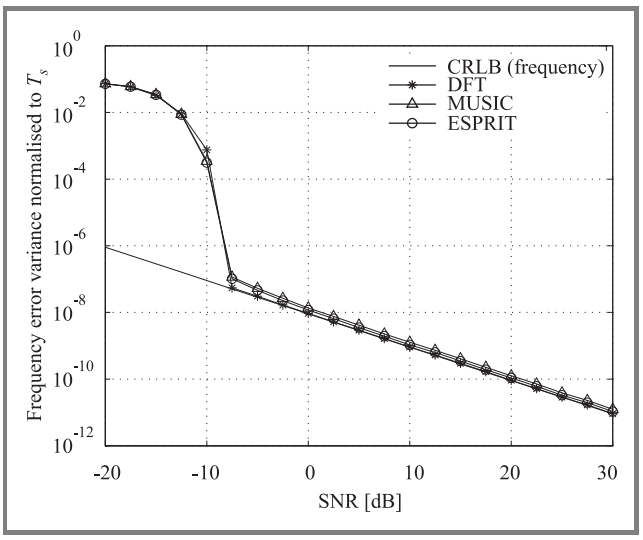


Fig. 2. The error variance of the DFT-based frequency estimator as a function of SNR.

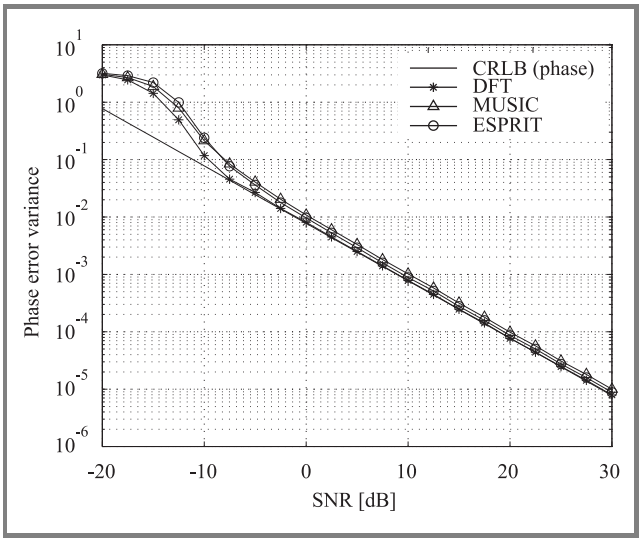


Fig. 3. The error variance of the phase estimator as a function of SNR.

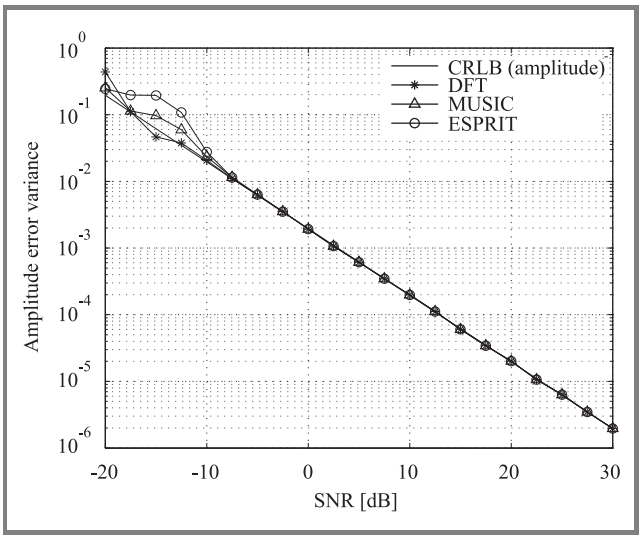


Fig. 4. The error variance of the amplitude estimator as a function of SNR.

quency, phase and amplitude estimator described in Section 2 compared to results obtained by the Matlab™ "rootmusic" algorithm and TLS-ESPRIT algorithm presented in [13]. The number of data points used in the simulation equals to 256 and the size of the autocorrelation matrix used for the "rootmusic" and TLS-ESPRIT algorithm equals to 64. For each trial a random frequency and phase is generated from two independent uniform distributions with the range $-f_s/2$ to $f_s/2$ and 0 to 2π, respectively. The results shown are obtained by averaging over 6000 trials. It can be seen that the simulated results obtained by the proposed algorithm is on par with those obtained by using "rootmusic" and TLS-ESPRIT and yet computationally very efficient.

Figure 5 shows a comparison of the frequency estimation error variance as a function of SNR between the modified

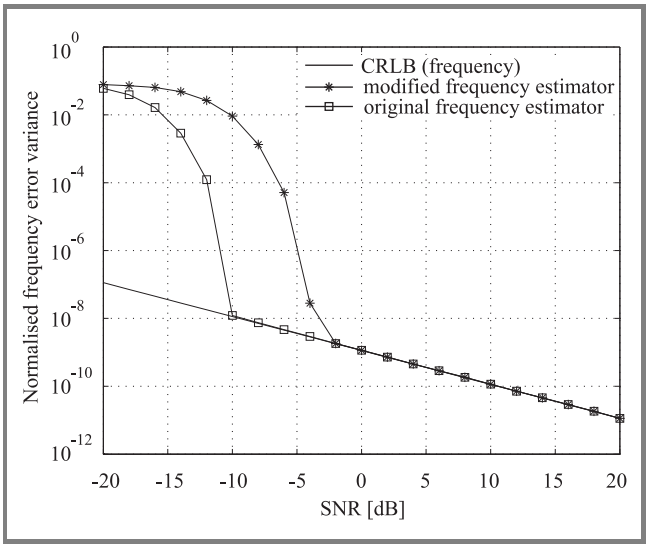


Fig. 5. The error variance of the modified frequency estimator compared to the original frequency estimator.

frequency estimator as described in Section 4 against the frequency estimator as described in Subsection 2.1. The frequency estimate obtained from two passes of the modified frequency estimator with $N_0 = 128$ and $N_1 = 512$. The number of samples was kept constant at $N = 512$ for the frequency estimator as described in Subsection 2.1. The results shown are obtained by averaging over 6000 trials. As expected, the modified version of the frequency estimator's performance threshold is at a higher SNR than the original estimator. However the modified frequency estimator only required $N_0 \log_2 N_0 + 4N_0 + 4N_1 = 3456$ complex multiplications which is approximately half of what is required for the original frequency estimator which equals to $N \log_2 N + 4N = 6656$ complex multiplications.

6. Conclusion

Expanding upon [1], a new algorithm for joint frequency, phase and amplitude estimation of a complex exponential

has been presented. It was shown that given sufficient number of samples, at high SNR the variance of the phase estimator approaches the asymptotic limit of 0.0475 dB above the CRLB. It was also shown that the modified version of the frequency estimator can significantly reduce the computation complexity with compromising the overall error variance performance except increasing the operation SNR threshold. With the advantage of being computationally efficient, this type of joint frequency and phase estimator is well suited for real time application such as timing and carrier synchronization.

Appendix

Variance of the DFT-based phase estimator

The arctangent of $r_{A,\theta}[n]$ as defined in Eq. (6) was given as

$$\hat{\theta}_{c,\hat{f}_m} = \tan^{-1}\left(\frac{\sum_{n=0}^{N-1} A\sin(2\pi\varepsilon n T_s + \theta_c) + \eta_s}{\sum_{n=0}^{N-1} A\cos(2\pi\varepsilon n T_s + \theta_c) + \eta_c}\right). \quad (24)$$

From [1], ε the frequency estimation error is a random variable with zero mean and variance of

$$Var[\varepsilon] = \frac{N\sin^2\left(\frac{\pi}{2N}\right)\tan^2\left(\frac{\pi}{2N}\right)}{4\pi^2 SNR}. \quad (25)$$

Again, the variance of $\hat{\theta}_{c,\hat{f}_m}$ in Eq. (24) can be found by using the technique of linearization of function of random variables presented in [8]. From the structure of the discriminate D_m defined in Eq. (4) one can conclude ε and η_c are uncorrelated and ε and η_s are uncorrelated. Expanding Eq. (24) in a three dimensional Taylor series expansion with respect to these variable gives

$$Var\left[\hat{\theta}_{c,\hat{f}_m}\right] = \left(\frac{\partial\overline{\hat{\theta}_{c,\hat{f}_m}}}{\partial\varepsilon}\right)^2 Var[\varepsilon] + \left(\frac{\partial\overline{\hat{\theta}_{c,\hat{f}_m}}}{\partial\eta_c}\right)^2 Var[\eta_c] + \left(\frac{\partial\overline{\hat{\theta}_{c,\hat{f}_m}}}{\partial\eta_s}\right)^2 Var[\eta_s], \quad (26)$$

where

$$\left(\frac{\partial\overline{\hat{\theta}_{c,\hat{f}_m}}}{\partial\varepsilon}\right) = \left(\frac{\partial\hat{\theta}_{c,\hat{f}_m}}{\partial\varepsilon}\right)\Bigg|_{\varepsilon=E[\varepsilon],\,\eta_c=E[\eta_c],\,\eta_s=E[\eta_s]} = \pi(N-1), \quad (27)$$

$$\left(\frac{\partial\overline{\hat{\theta}_{c,\hat{f}_m}}}{\partial\eta_c}\right) = \left(\frac{\partial\hat{\theta}_{c,\hat{f}_m}}{\partial\eta_c}\right)\Bigg|_{\varepsilon=E[\varepsilon],\,\eta_c=E[\eta_c],\,\eta_s=E[\eta_s]} = -\frac{\sin(\theta)}{NA}, \quad (28)$$

$$\left(\frac{\partial\overline{\hat{\theta}_{c,\hat{f}_m}}}{\partial\eta_s}\right) = \left(\frac{\partial\hat{\theta}_{c,\hat{f}_m}}{\partial\eta_s}\right)\Bigg|_{\varepsilon=E[\varepsilon],\,\eta_c=E[\eta_c],\,\eta_s=E[\eta_s]} = \frac{\cos(\theta)}{NA}. \quad (29)$$

Solving Eq. (26) yields

$$Var\left[\hat{\theta}_{c,\hat{f}_m}\right] = \frac{N^2(N-1)^2\sin^2\left(\frac{\pi}{2N}\right)\tan^2\left(\frac{\pi}{2N}\right)+2}{4N\,SNR}. \quad (30)$$

Acknowledgements

The authors would like to thank the Australian Cooperative Research Center for Satellite Systems and the University of Technology, Sydney, for their funding and support. The work was funded in part by the Commonwealth Government of Australia through the Cooperative Research Centers Program.

References

[1] S. Reisenfeld, "A highly accurate algorithm for the estimation of the frequency of a complex exponential in additive Gaussian noise", in *5th Austr. Commun. Theory Worksh.*, Newcastle, Australia, 2004, pp. 154–158.

[2] S. Reisenfeld and E. Aboutanios, "A new algorithm for the estimation of the frequency of a complex exponential in additive Gaussian noise", *IEEE Commun. Lett.*, vol. 7, issue 11, pp. 529–551, 2003.

[3] D. C. Rife and R. Boorstyn, "Single tone parameter estimation from discrete-time observations", *IEEE Trans. Inform. Theory*, vol. IT-20, no. 5, pp. 591–598, 1974.

[4] S. Kay, "A fast and accurate signal frequency estimator", *IEEE Trans. Acoust., Speech Sig. Proces.*, vol. 37, no. 12, pp. 1987–1990, 1989.

[5] R. Schmidt, "Multiple emitter location and signal parameter estimation", *IEEE Trans. Anten. Propagat.*, vol. 34, no. 3, pp. 276–290, 1986.

[6] R. Roy and T. Kailath, "ESPRIT – estimation of signal parameters via rotational invariance techniques", *IEEE Trans. Acoust., Speech Sig. Proces.*, vol. 37, no. 7, pp. 984–995, 1989.

[7] S. M. Kay, *Fundamentals of Statistical Signal Processing Estimation Theory*. Upper Saddle River: Prentice Hall, 1993.

[8] *Problems in Probability Theory, Mathematical Statistics and Theory of Random Functions*, A. A. Sveshnikov, Ed. New York: Dover, 1968.

[9] B. James, B. D. O. Anderson, and R. C. Williamson, "Characterization of threshold for single tone maximum likelihood frequency estimation", *IEEE Trans. Sig. Proces.*, vol. 43, pp. 817–821, 1995.

[10] A. O. Steinhardt and C. Bretherton, "Thresholds in frequency estimation", in *Proc. ICASSP*, Tampa, USA, 1985, vol. 10, pp. 1273–1276.

[11] B. G. Quinn and P. J. Kootsookos, "Threshold behavior of the maximum likelihood estimator of frequency", *IEEE Trans. Sig. Proces.*, vol. 42, pp. 3291–3294, 1994.

[12] L. Knockaert, "The Barankin bound and threshold behavior in frequency estimation", *IEEE Trans. Sig. Proces.*, vol. 45, pp. 2398–2401, 1997.

[13] D. G. Manolakis, V. K. Ingle, and S. M. Kogon, *Statistical and Adaptive Signal Processing – Spectral Estimation, Signal Modelling, Adaptive Filtering and Array Processing*. Boston: McGraw Hill, 2000.

Jeffrey Tsui received his B.E. degree in telecommunication engineering the University of Technology, Sydney, in 2002. He is currently a final stage Ph.D. student at the University of Technology, Sydney. His research interests include signal processing and its applications in the areas of satellite communication and wireless communication technologies.
e-mail: jtsui@eng.uts.edu.au
Faculty of Engineering
Cooperative Research Center for Satellite Systems
University of Technology, Sydney
PO Box 123, Broadway, NSW 2007, Australia

Sam Reisenfeld received the B.Sc. degree in information engineering specializing in communication systems engineering from the University of Illinois in 1969 and the M.Sc. and Ph.D. degrees in communication systems engineering from UCLA in 1972 and 1979, respectively. From June, 1969 until September, 1988, he was a space communication systems engineer at the Hughes Aircraft Company, Systems Laboratories, Space and Communications Group, El Segundo, California. From September, 1988 until the present, he is an Associate Professor of telecommunication engineering at the University of Technology, Sydney, Australia. From January, 1997 until the present, he also is the Program Director for Ka band Satellite Communications Research and Development in the Australian Cooperative Research Centre for Satellite Systems. He is a Member of Phi Kappa Phi and the IEEE. He received the IEEE Millennium Medal in November, 2000.
e-mail: samr@uts.edu.au
Faculty of Engineering
Cooperative Research Center for Satellite Systems
University of Technology, Sydney
PO Box 123, Broadway, NSW 2007, Australia

Regular paper

Future automation via ubiquitous communications technologies

Eduard Babulak

Abstract— The telecommunications and Internet technologies have evolved dramatically during the last decade, laying solid foundation for the future generation of the ubiquitous Internet access, omnipresent web technologies and ultimate automated information cyberspace. As a result, current efforts in the research and development in the areas of next generation of Internet and telecommunications technologies promote formation of inter-disciplinary international teams of experts, scientists, researchers and engineers to create a new generation of applications and technologies that will facilitate the fully-automated information cyberspace systems, such as future house 2015. The author discusses the current state of the art in the world of telecommunications and Internet technologies, new technological trends in the Internet and automation industries, as well as the concept of the fully-automated future house 2015, while promoting research and development in the inter-disciplinary projects run by multinational teams world-wide.

Keywords— automation, cyberspace, smart house, ubiquity, convergence.

1. Introduction

The past 20th century left us with legacy of the global Internet, final flight of the Concorde airliner, CISCO monopoly in computer networking, etc., while large, medium and small corporations alike have discovered the need to adapt to the new technologies, or sink in the emerging global knowledge economy. There is no facet of life in the industrialized world that has not undergone some form of shift. The resultant new information economy has brought with it different approaches to work. The current 21st century is perhaps one of the most interesting times in history to be alive. We are witnessing a phenomenal abundance of change in societies around the world in a very short period. The source of most of this change is new technologies and the Internet. In the past decade we have seen every aspect of the lives of individuals and organizations go through many evolutions and uncertainties [1]. There are plenty of publications on the subject of futuristic and ubiquitous computing for the 21st century presenting excellent discussion and possible scenarios in the subject area [2–6].

History proved that one must look forward and accept the futuristic vision as possible scenarios of tomorrow's reality. Nowadays, technologies such as TV, Internet, mobile phone, traffic lights, cameras are essential part of daily life. However, if one would suggest hundred years ago what would be the reality of 2005, surely he or she would be considered "with great caution" [13, 14]. Past 20th century gave rise to new technologies that have become a reality for us all. Today, we are yet again at the very beginning of evolution of even more advanced and sophisticated technologies. Current industries, governments, business, academic and research institutions are all computerised and interconnected via Internet.

2. Pervasive computing

Research and development trends in the filed of computing industry promote a vision of smart spaces, smart devices, clothing, fully automated houses, etc., which creates an environment where computers are everywhere and provide ultimate access to Internet. Pervasive computing environments, such as the ones studied in CMU's Aura project [15], provide many kinds of information. Some of this information should be accessible only by a limited set of people. For example, a person's location is a sensitive piece of information, and releasing it to unauthorized entities might pose security and privacy risks. For instance, when walking home at night, a person will want to limit the risk of being robbed, and only people trusted by the person should be able to learn about her current location.

The access control requirements of information available in a pervasive computing environment have not been thoroughly studied. This information is inherently different from information such as files stored in a file system or objects stored in a database, whose access control requirements have been widely studied. The market is evolving from wired computing to pervasive computing, mobile and wireless, anytime at anyplace. Many types of information available in a pervasive computing environment, such as people location information, should be accessible only by a limited set of people. Some properties of the information raise unique challenges for the design of an access control mechanism. Information can emanate from more than one source, it might change its nature or granularity before reaching its final receiver and it can flow through nodes administrated by different entities [16].

New developments in telecommunications industry gave rise to embedded systems working as networks. Many embedded systems today may be characterized as computing network, while chip architectures will follow the network-on-chip paradigm. Devices such as mobile terminals will have a distributed communication centric architecture, while hardware (HW) and software (SW) development for such systems will be communications centric. This will be a paradigm shift and a major challenge for the engineering community especially for SW developers,

since traditional SW programming methods do not work well for distributed highly concurrent platforms.

3. Commerce and automation

Current research efforts in automation industry are inspired by manufacturing evolution which went from heavy engineering plants in UK on 19th century to 20th century modern manufacturing concepts, while entering completely new dimension in the world of Internet and electronic information interchange world-wide. The manufacturing and automation technologies have cross the frontiers from nanotechnology to giga networks infrastructures that are essential in enabling the information flow between robots, powerful computing centres and man controlled stations. The current merger of current computer integrated manufacturing technologies and data-telecommunications technologies present a new challenge to community of engineers and scientists in the manufacturing sector as well as, mathematics and computing science and engineering sector [17–19]. The economic prospects for 2005/10 remain particularly hard to predict. Whilst the markets for control and power industry proved to be challenge for the companies, the software and automation industry have grown, particularly those businesses serving the oil, gas, power generation and auto markets [17]. What gives rise to pressures in the market place are company drivers in conjunction with the industry drives.

Globalization of the market with accelerating technological changes such as digital revolution and mobile technologies in conjunction with the customer demands represent main industrial drivers [20]. On the company site it is the cost efficiency combined with the new lines of products that give rise to business complexity. The major forces in industry today are e-commerce and e-manufacturing [7]. E-manufacturing has been well adopted in industry overseas and the next wave of the e-manufacturing is driven by customers utilizing full capacity of e-commerce [8]. Toyota is one of many examples where e-manufacturing has become a major force for their productivity and business success.

Future technological advancements open a new avenue for multidisciplinary development and research teams consisting of IT professionals such program developers, telecommunications engineers, production engineers and business managers to work closely with academics and industrial research teams on new e-manufacturing solutions. Sales marketing forces combined with the manufacturing and operation teams work together to plan the dynamics for future vision and the current reality, while facilitating supply chain of products in respond to customer chaotic orders. As a result, real-time planning and execution must be well balanced with the plant chaos. Both processes of making order and forecast are reflected well in the domain of vision and the reality while main facilitator for the customer remains to be Internet world-wide. Customers order behavior with mobility represents very complex, dynamic and nonlinear systems [9]. A firm's ability to serve its customers needs determines its success. Initially, firms needed to meet face-to-face to meet most of their customer's needs; however, with the development of information technology, the requirement for face-to-face interaction has gradually declined.

The Internet opened up a new channel for firm-customer interaction that has significantly changed the customer relationship equation. Now, cell phone networks are enabling m-commerce and further change in the firm-customer dynamics [21]. Traditionally, business has been biased by geography and located near rivers, roads, and other transport services so that the cost of being reached by customer or reaching customers is lowered. Now, business is increasingly using electronic networks (e.g., the Internet and mobile phone networks) to interact with customers. Thus in the next few years, it is likely that we will see the emergence of u-commerce, where u stands for ubiquitous, universal, unique, and unison. U-commerce is the use of ubiquitous networks to support personalized and uninterrupted communications and transactions between a firm and its various stakeholders to provide a level of value over, above, and beyond traditional commerce. U-commerce represents the use of ubiquitous networks to support personalized and uninterrupted communications and transactions between a firm and its various stakeholders to provide a level of value over, above, and beyond traditional commerce.

Ubiquitous represents concept of having [21]:

- networks everywhere;
- all consumer durable devices are on a network;
- intelligence and information are widely dispersed and always accessible;
- smart entities;
- appliances:
  - buildings,
  - signs,
  - street smart communities.

The main focus is to enable one global network that would be available 24 hours a day, seven days a week, whole year round and will provide best quality of services to anyone, anywhere and anytime. World's telecommunications providers are looking for the ways to merge together all digital and analogue services (voice, video, data) on one common network, which would provide users with unlimited access to online information, business, entertainment, etc. Convergence's goal is to provide corporations with a highly secure and controllable solution that supports real-time collaborative applications [10].

4. Smart house 2005 scenario

In last decade, number of researcher articles presented vision and illustrated the scenarios of futuristic computing systems in the year 2005 [18]. Today, we are in the begin-

ning 2006 and much of the foreseen technology is already implemented and fully integrated in industry, military, businesses, education and home.

Mark Weiser in his article written in 1996 wrote about futuristic computer technologies applied in "smart house in the year 2005" [14]. Mark Weiser's vision did indeed materialised and some of his concepts are currently ongoing research and implementation projects. Ultimately the ubiquitous computer and Internet technologies should make living more comfortable for all. Looking back at my own graduation in London in 1991, I remember a statement made by the distinguish Professor of computer science who was awarded the Doctor of science degree. He said: "Computer technology today has influenced almost every aspect of our lives, industry, business, education. However, most unfortunately computer technology have mechanised the relationship between people due to e-mail and Internet technologies. It is important that the research, academic and industrial community work together to reverse that equation, whereby computer technology will be a tool that will improve human lives and mutual interaction". Author encourages reader to reflect on that statement.

Let us imagine scenario where you and I will live in the "smart house 2015". Early morning, just before the sunrise the fridge will send a message to local milkman, baker and fruit-vegetable market to make sure that breakfast will be served as usual with five star quality. While fridge completes its duties for the rest of the day and order all fresh food necessary for the day, the local information house center will make sure that dining room is ready (i.e., silent vacuum cleaner and window washer completed it's job just before the sunrise). Garden is tendered everyday, garage is looking after car, making sure that batteries are fully recharged and that heat fits with the local weather forecast. Chairs, table, all kitchen appliances are ready and in place. Son after breakfast they will proceed with self cleaning, self storage. The local information health centre will examine the hygiene in the house and diagnose all possible viruses that are in the area and in the work place. All necessary vitamins and medications will be administered automatically and painlessly. For those who are overweigh if agreed to in-house regime policies, food chain calories will be carefully supervised and monitored by fully automated cook and service appliances. Every member of the family will have automatically prescribed the educational and entertainment programs according to their position (i.e., pupil, student, engineer, academic, worker, etc.). In addition, the local heath centre will monitor house members' state of health per 24 hours, every day, consult the medical database and automatically alert the house member and local doctor in case of urgency. Naturally, there are issues related to the house automatic positioning systems and security systems, which will be carefully monitored and controlled remotely by the house owner or if necessary by the local weather centre. In case of natural disasters these systems will protect the house and its members while switching to contingency plan B. Well, all we need is to wait until 2015 and see if this vision will materialise.

Fully automated environment will require sophisticated MIMO antenna systems and small smart devices that will be able to communicate within themselves all the time. These devices will have self healing capabilities to make sure that they are recharged regularly and will be operational without any interruption. Similar to us humans we have breakfast, lunch, dinner and snack on accession to make sure that we are able to do our job, and yet we sleep anywhere from 6 to 14 hours each day. Device creating the fully automated space can not sleep, perhaps they may wait or be on pause mode, but as soldiers they must be in full operational readiness at any time and anywhere.

The advancement of current technologies in the fields such as data and telecommunications, ubiquitous Internet access and sensor technologies combined with the new revolutionary explorations and concepts in biotechnology and nano-technology, computer human interface-interaction, etc., present a great challenge for the research community not only as a result of mathematical complexity, but most of all by the user's perception [22]. It is essential to remember that technology is only a tool an utility resource that is available to us all. Did we find the answer to simple question such as:

- Why it is that if little spider falls from the table down on the kitchen floor, it never breaks its tiny legs?
- Did we really make progress in automation and if yes to what extend?
- What is the ultimate Internet access?
- What is the truly intelligent fully-automated cyberspace?

5. Conclusion

Automation did inspire number of outstanding scientists and engineers in the past centuries to find new solution to ease lives for all mankind. The emergence and accessibility of advanced data and telecommunications technologies combined with convergence of industry standards, as well as the convergence of data and telecommunications industries contribute towards the ubiquitous access to information resources via Internet [11, 12].

The automated environment and cyberspace systems for the 21st century entered a new era of innovation and technological advancements. World's industry and commerce are becoming more and more computerised having a global vision for the future. With increased benefits and improvements in overall information technology, the benefit-to-cost ratio has never been higher. It is essential to continue in the developments of industry standards and application of information technologies in order to increase the automation and ultimate success of modern logistics, the e-commerce and e-manufacturing industries [23, 24].

The automated environment and cyberspace systems for the 21st century entered a new era of innovation and technological advancements. World's industry and commerce are becoming more and more computerized having a global vision for the future.

Author presents his own vision on future automated environment via information cyberspace for the year 2015. Paper suggests the integration of automated environments and intelligent cyberspaces in light of applied robotics, logistics, smart devices, smart antennas and intelligent systems. Author hopes that this paper will encourage the research and industrial community to invest their efforts in implementing fully automated environments via intelligent cyberspaces. Future efforts should be focused on designing a communication language and transmission media that will allow for instantaneous communication transfer and control between smart devices and humans.

Current research and development efforts in the areas of industrial automation, robotics and Internet bring together large team of researcher and experts worldwide. Telecommunications and data networks infrastructures are the essential platform for industrial automation and Internet.

The promotion of interdisciplinary activities in the areas of informatics, engineering, mathematics, as well as, aesthetics and business is quickly becoming one the most exiting fields of academic and industrial research.

References

[1] Government Canada, http://www.atirtf-geai.gc.ca/submissions/riley2001-05-30-f.html

[2] Security for ubiquitous computing, http://www-lce.eng.cam.ac.uk/ fms27/secubicomp/index.html

[3] Ubiquitous computing, http://www.ubiq.com

[4] Ubiquitous computing, http://www.cs.albany.edu/ maniatty/teaching/ubicomp/index.html

[5] Ubiquitous computing, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

[6] Bleutooth, http://www.bluetooth.com

[7] Advanced manufacturing research, http://www.amrresearch.com/

[8] Toyota, http://www.toyota.com/

[9] Agile manufacturing concepts, http://www.darpa.mil/mto/solicitations/CBD/cbd_9431A.html

[10] Convergence, http://www.covergence.com/contact.html

[11] IEEE pervasive computing, http://www.computer.org/pervasive

[12] PERVASIVE computing © 2005 IEEE, published by the IEEE CS and IEEE ComSoch, http://www.computer.org/portal/site/pervasive

[13] F. Stajano, *Security for Ubiquitous Computing.* New York: Wiley, 2002.

[14] M. Weiser, "Open house". Web magazine of the Interactive Telecommunications Program of New York University, 1996, ITP, Review 2.0, http://www.itp.tsoa.nyu.edu/∼review/

[15] D. Garlan, D. Siewiorek, S. Smailagic, and P. Steenkiste, "Project Aura: towards distraction-free pervasive computing", *IEEE Perv. Comput.*, vol. 1, no. 2, pp. 22–31, 2002.

[16] U. Hengartner and P. Steenkiste, "Protecting access to people location information", in *Proc. Int. Conf. Secur. Perv. Comput. SPC'2003*, Boppard, Germany, 2003.

[17] E. Babulak, "Manufacturing for the 21st Century", in *1st Int. Conf. Manufact. Manag.*, Presov, Slovakia, 2004.

[18] E. Babulak, "Automated environment via cyberspace", in *Int. Conf. Appl. Comput. IADIS 2005*, Algarve, Portugal, 2005.

[19] E. Babulak, "Quality of service provision assessment in the healthcare information and telecommunications infrastructures", selected for publication in the *Int. J. Med. Inform.*, Elsevier Ireland, 2005.

[20] H. Wohlwend, "An e-factory vision", in *2nd Eur. Adv. Equip. Contr./Adv. Proc. Contr. Conf.*, Dresden, Germany, 2001.

[21] R. T. Watson, *Data Management: Databases and Organizations*, 4th ed. New York: Wiley, 2004.

[22] E. Babulak, "Next generation of Internet and telecommunications technologies for fully automated cyberspace", in *7th Int. Conf.* "New Trends in Technology System Operation", Presov, Slovakia, 2005.

[23] *Third International Conference, PERVASIVE 2005*, H. W. Gellersen, R. Want, and A. Schmidt, Eds. *Lecture Notes in Computer Science*. Springer, 2005, vol. 3468.

[24] B. Shade, *Increased Productivity Through E-Manufacturing.* Cahners Business Information, Advanced Energy Inc., Fort Collins, Colorado, USA, 2001.

Eduard Babulak – Professor, Ph.D., P.Eng., Eur.Ing., C.Eng., C.IT.P, SMIEEE – worked as a University Professor, Senior Lecturer and Researcher in mathematics, electrical, computer engineering and computing science in Canada, USA and United Kingdom. He speaks 14 languages and was nominated to a Fellow of British Computer Society (BCS) and a Fellow of the Association of Computer Machinery (ACM). He is a Senior Member of IEEE, a Corporate Member of IEE, a Professional Member of BCS, a Professional Member of ACM, a Member of American Society for Engineering Education (ASEE), American Mathematical Association (AMA) and a Member of the Mathematical Society of America (AMS). He is an international scholar, researcher, consultant, educator, professional engineer and polyglot with more than twenty two years of teaching experience and industrial experience as a professional engineer in USA, Canada, UK, Germany, Austria, and Czech Republic and Slovakia. Professor Babulak's biography was selected for citation in the Cambridge Blue Book 2005, the Cambridge Index of Biographies 2004 and 2005, the Dictionary of International Biography 2004, published by the Cambridge Center of International Biographies, Who is Who in the Science and Engineering 2003, 2004 and 2005, Who is Who in the Industry and Finance 2004 and 2005 and in the Who is Who in the World 2003 and 2004. Professor Babulak's academic and engineering work was recognized internationally by the Engineering Council in UK and European Federation of Engineers. His academic qualifications have been recognized and credited by the Association of Professional Engineers of Canada in Toronto. His research interest is in human-centric and ubiquitous computing, e-manufacturing, QoS provision for computer and telecommunications communications infrastructures, differentiated networks, health informatics, electronic health record, automation and applied mathematics.

e-mail: babulak@ieee.org

Faculty of Computing and Engineering Technology

Staffordshire University

Beaconside, Stafford, ST18 0DG, United Kingdom

Regular paper

Reliability of line-of-sight radio-relay systems

Jan Bogucki and Ewa Wielowieyska

Abstract— The modern radio transmission systems are specifically designed for catching principally two main objectives: on one side to provide a radio solution for long distance where large configurations are required to fulfill the high capacity transmissions needs, on the other side to guarantee link quality as high as possible. The availability of a radio-relay system is dependent upon many factors and particularly upon: the reliability of equipment and propagation conditions. The article describes the wave propagation and equipment that determine the performance of a radio-relay path. National Institute of Telecommunications (NIT) carried out research on propagation phenomena on terrestrial path and exemplary results are described herewith. The availability of radio equipment based on the mean time between failures for equipment modules is presented too.

Keywords— line-of-sight radio links, propagation, equipment, reliability.

1. Introduction

Time operation of radio links is split into two periods, when it is in working order or out of order. Radio links are out of order when even one of its basic parameters is crossing permissible limit spread. This occurrence is called failure. It is not essential the failure to follow rapidly or gradually. The total unavailability of radio path is the sum of the probability of hardware failure and unavailability due to propagation conditions.

There are six transmission parameters, which may be used to characterize of unsatisfactory quality performance. These are bit error ratio (BER) or frame error rate (FER), short interruption, delay, jitter, slip and quantizing noise. The ratio BER/FER and short interruption are the main indicators of unavailability. This is because jitter and slip will cause bit errors and short interruption in the network and that delay and quantizing noise are relatively fixed quantities in any connection.

Line-of-sight radio-relay systems are defined unavailable when one or both of the following conditions occur for more than 10 consecutive seconds:

- the digital signal is interrupted,
- the BER in each second is worse than 10^{-3}.

It should be noted that the unavailability for system has to be considered for both "the go" and "the return" direction, that is twice the calculated value.

2. Link availability (reliability)

Many fixed broadband wireless links are designed to be available essentially at all times. Available A means that BER or FER is at or below a given quality threshold level:

$$A\ [\%] = \frac{100\ (total\ usage\ time - downtime)}{total\ usage\ time}.$$

Conversely, an outage is the time when the link is not available. An outage of only 53 mines a year is an availability of 99.99%. The availability percentage is usually based on an annual average although link outage due to fades is normally calculated on a worst month basis.

The annual outage time is simply related to percentage availability by:

$$outage\ time = \left(1.0 - \frac{percent\ availability}{100}\right) 525600\ \text{min}.$$

An outage can occur for a variety of reasons, including multipath fades, rain fades, diffraction fades and equipment failures. Calculating the probability that fades of a particular magnitude occur, or equipment failures occur, will lead directly to the probability of an outage and hence the link availability probability.

3. Causes of unavailability

The availability of a radio-relay system is dependent upon many factors and particularly upon: the maintenance organization (which determines the time to restore), the reliability of equipment's and the system design and propagation conditions. The relative importance of these various factors may vary significantly, sometimes without possibility of control, from one area to another.

System planners should take into account all causes of interruption or quality degradation affecting system unavailability. Features of the major causes of unavailability in radio-relay systems are described below.

Equipment. Estimate of unavailability should include all causes which are statistically predictable, unintentional and resulting from the radio equipment. Such causes can be as follows:

- failure or degradation of radio equipment including modulators and demodulators,
- failure of auxiliary equipment such as switch-over equipment,
- failure of radio system power supply equipment,
- failure of antenna or feeder.

Propagation. System interruptions due to deep multipath fading often recover within 10 s, however, they sometimes occur for more than 10 s causing unavailability. Excessive precipitation-attenuation due to heavy rainfall or snow fall lasts for a fairly long time and causes unavailability in systems operating in the frequency bands above 10 GHz. Fading due to layering of the atmosphere is the dominating factor of degradation of radio-relays in the frequency bands below 8 GHz. It may be possible to derive prediction statistics on propagation effects by applying the formulae or methods given in [4] and [5]. Also, since there is generally a low probability of heavy precipitation occurring, the unavailability time it causes may differ from year to year.

Diffraction fades. When there are two radio antennas located on or near the Earth's surface propagation can ordinarily occur between them by groundwave. If an obstruction, a hill, a mountain, a building intervenes, propagation can still occur via slant paths over the top edge of the obstruction. This depends on diffraction over the edge. There is an additional loss due to diffraction. For zero diffraction loss the direct line of sight path between transmitter and receiver must clear the obstruction by several wavelengths. When the direct path just grazes the obstruction diffraction loss is exactly 6 dB.

Other causes. Unpredictable noise bursts due to interference mainly from sources outside the interfered with system may cause unavailability when the noise power exceeds a certain threshold. This kind of interruption includes interference from space systems or radar systems associated with anomalous propagation. Human intervention during maintenance activities can also cause unavailability.

4. Propagation affects error performance and availability objectives

Fading due to condition of the atmosphere is the dominating factor of degradation of radio-relays. Fading (being random variable) can cross threshold only in specific period of time. Fading events are mainly caused by multipath in range of frequency below 8 GHz and by precipitation in range above 20 GHz. Definition probability of appearance those events are great of importance on reliability of line-of-sight radio-relay systems.

Transmission of microwave signals above 10 GHz is vulnerable to precipitation. The attenuation due to absorption is larger than attenuation due to scatter for wavelengths that are until compared with the drop size. For wavelengths that are short compared to drop size, the attenuation due to scatter is larger than due to absorption.

Multipath fadings are especially dangerous in high capacity systems, where signal spectrum occupied comparative frequency wide band. Formulas mathematical describing these phenomena are given in [4] and [5]. Meteorological conditions in the space separating the transmitter and the receiver may sometimes cause detrimental effects to the received signal. Rays that normally would have been lost in troposphere may be refracted into the receiving antenna where they are added to the wanted signal. The phase- and amplitude-relationship between signals determines the resultant input signal at the receiver. Multipath fadings triggering off deep notch in transfer function of radio links cause the increasing BER because of that:

– decreasing signal to noise ratio,

– decreasing signal to interference ratio,

– decreasing separation between two orthogonal components I and Q.

The prevision of attenuation which may arise in the radio link channels are due to multipath and atmospheric precipitation demanding knowledge of either the probability distribution of precipitation intensity or of the probability distribution condition propagation along the determined routes. Taking into consideration the nature and the necessity of research on propagation effects occurring in radio links, detailed instructions and requirements, which should be met to prepare self-operating measuring position, have been described in [2, 5]. Furthermore such position has been produced and set-up to work with radio links receivers. The radio links have been developed to test propagation in band X, Ka and Q. This paper describes the example tests results of wave attenuation in above mentioned radio links.

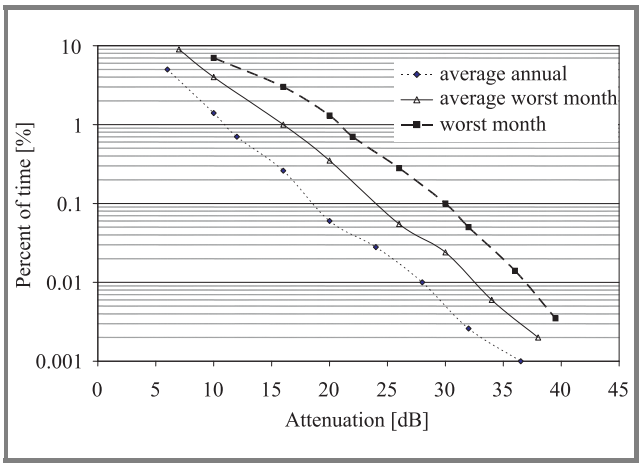


Fig. 1. The average worst month and the worst month attenuation distributions in 5-year period in comparison with the average annual distribution for 6 GHz and 52.3 km route.

For example, Fig. 1 shows the average worst month and the worst month attenuation distributions in 5 year-period in comparison with the average annual distribution for 52.3 km route. At the National Institute of Telecommunication (NIT) it has been researched into precipitation fading on line-of-sight radio links too.

For example, Fig. 2 shows 18.6 GHz frequency and 15.4 km route in 2-year period.

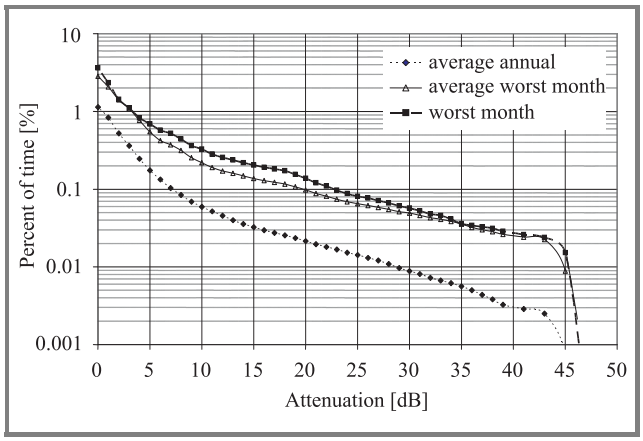


Fig. 2. The average worst month and the worst month attenuation distributions in 2-year period in comparison with the average annual distribution for 18.6 GHz and 15.4 km route.

Atmospheric disturbances affect the transmission conditions for the line-of-sight radio-relay systems. The received signal will vary with time and the system performance is determined by the probability for the signal level drop below the radio threshold level or the received spectrum to be severely distorted. Hence it is important to choose optimal frequency for working radio link, its diameters of parabolic antennas, transmitter power and receiver characteristic. In order to estimate the performance of a radio link system, a link power budget has to be prepared. The difference between nominal input level and radio threshold level, the fading margin are the main input parameters in the performance prediction model.

Table 1

Power budget of radio links 6 GHz and 18 GHz

Parameters	6 GHz, 50 km	18 GHz, 15 km
Transmitter output power [dBm]	+20	+20
Feeder loss transmitter [dB]	1	1.2
Branching loss [dB]	1.5	1.6
Transmitter antenna gain [dB]	39	45.2
Free space loss [dB]	142	141
Receiver antenna gain [dB]	39	45.2
Feeder loss receiver [dB]	1	1.4
Nominal input level [dB]	–43.5	–36.4
Receiver threshold [dB]	–71	–70
Fading margin [dB]	–27.5	–33.6

Nominal input level means power on input receiver for normal propagation condition, i.e., without attenuation due to multipath or precipitation.
Lets consider typical radio link capacity STM-1 (Table 1):

– 6 GHz frequency, 50 km path length, 1.8 m diameters of parabolic antennas;

– 18 GHz frequency, 15 km path length, 1.2 m diameters of parabolic antennas.

The link budget for the radio links of 50 km path and 6 GHz frequency is shown on Fig. 3. In comparison the results

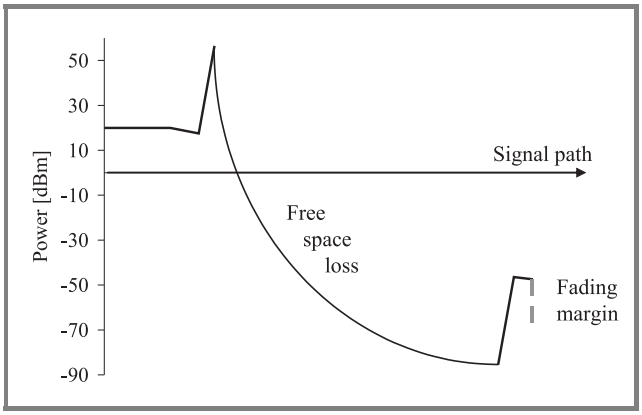


Fig. 3. Transmit/receive system and its link budget.

power budget with data on Fig. 1 it can be affirmed this fading margin assures 0.21% in the worst month, i.e., 0.42% duplex transmission. In comparison the results power budget with data on Fig. 2 it can be affirmed this fading margin assures 0.04% in the worst month, i.e., 0.08% duplex transmission.

5. Equipment failure rate

The probability that electronic equipment fail is not constant with time. Initial and wear-out failures give higher probability during the burn-in and wear-out periods. We concentrate on the useful lifetime where random failures give a constant probability.
After the burn-in period, the equipment failure rate is assumed to be constant until the wear-out period starts, and the equipment reliability can be predicted using analytical methods. If the failure rate is λ, the probability of m failures when testing n equipment modules in a unit time is given by the binomial distribution:

$$p_m = \frac{n!}{m!(n-m)!}\lambda^m(1-\lambda)^{n-m}. \tag{1}$$

The mean value of this distribution is given by

$$\sum_{m=0}^{n} p_m m = n\lambda. \tag{2}$$

The average number of surviving equipment modules after unit time is given by

$$N_{av} = n - n\lambda\,. \tag{3}$$

The number of surviving equipment modules vary with time t on average and is given by

$$n = n_0 \mathrm{e}^{-\lambda t}\,, \tag{4}$$

where n_0 is initial number of equipment modules.

A constant failure rate gives an exponential decrease of surviving equipment modules.

Mean time between failures. If the failure rate per unit time equals λ, the mean time between failures (MTBF) T_{av} is Δt:

$$\Delta t = \frac{1}{\lambda}\,. \tag{5}$$

Calculation of unavailability. Mean time between failures $T_{av} = \Delta t$ is more convenient to use than λ when calculating unavailability. The unavailability of one equipment module (Fig. 4a) is given by

$$N_1 = \frac{T_{n_0}}{T_{av} + T_{n_0}}\,, \tag{6}$$

where T_{n_0} is mean time to repair (MTTR).

For telecommunication equipment:

$$T_{av} \gg T_{n_0} \tag{7}$$

and Eq. (6) may be approximated by

$$N_1 = \frac{T_{n_0}}{T_{av}}\,. \tag{8}$$

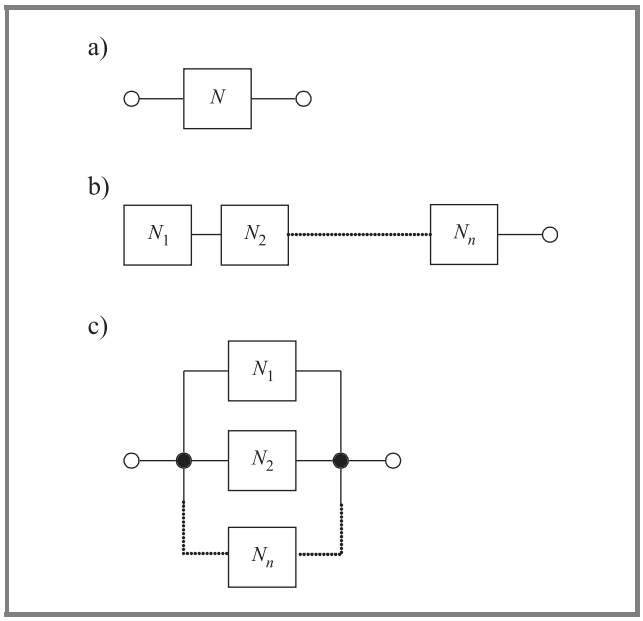


Fig. 4. One equipment module (a), cascaded modules (b) and parallel modules (c).

Unavailability of cascaded modules. The system in Fig. 4b will be available only if all the modules are available simultaneously. The availability of the total system is given by

$$A_s = \prod_{j=1}^{n} A_i = \prod_{i=1}^{n} (1 - N_i)\,. \tag{9}$$

The corresponding unavailability is given by

$$N_s = 1 - A_s = 1 - \prod_{i=1}^{n} (1 - N_i) \approx 1 - \left[1 - \sum_{i=1}^{n} N_i\right] = \sum_{i=1}^{n} N_i\,. \tag{10}$$

So, when the unavailability is much smaller than availability, the unavailability of a system of cascaded modules is the sum of the unavailability's of its individual modules.

Unavailability's of its individual modules. Modules may be connected in parallel. The system will then unavailable only if the modules are unavailable simultaneously. The unavailability is given by

$$N_s = \prod_{i=1}^{n} N_i\,. \tag{11}$$

Protection switching. Continuous monitoring of digital radio-relay system is necessary for initiating protection switching under conditions of channel failure. Protection switching is often effective to improve system availability. In radio-relay systems the so-called multi-line switching method is usually used. In this method one or r ($r > 1$) protection radio channels are prepared for k working channels. When one of the k working channels is interrupted the signal in the interrupted channel will immediately be recovered by one of the protection channels over s radio hops. In such a case, the unavailability N of each both-way radio channels due only to equipment failure, assuming that the failure rate of switching equipment is negligibly small, can be expressed by the following formula:

$$N = \frac{2}{k}\left[\binom{k+r}{r+1}\right](sU)^{r+1}\,, \tag{12}$$

where s is number of radio hops contained in a switching section and U is probability of an interruption of each hop (as far as equipment failure is concerned, U = MTTR/MTBF):

$$\binom{k+r}{r+1} = \frac{(k+r)!}{(r+1)!(k-1)!}\,. \tag{13}$$

In many cases the number of the protection channels $r = 1$ and formula (12) can be written by the following:

$$N = \frac{2}{k}\left[\binom{k+1}{2}\right](sU)^2\,. \tag{14}$$

Protection switching is effective not only for equipment failure but also for multipath fading through frequency diversity.

Equipment failures of modern radio links. The latest radio-relay systems are designed to be highly reliable and the MTBF becomes extremely long. For high reliability link systems that must have outages of only a few minutes a year, equipment failure can play an important part in achieving this reliability. Equipment failure can come from component failure in the equipment itself or physical damage to the equipment from violent weather or vandalism. If a microwave relay site is on a remote mountaintop, access by road or even by helicopter to repair a problem can take several hours or longer. A single such failure alone may violate the reliability objective of the system. The equipment reliability is usually given as MTBF. This is a published equipment specification that varies from 50 000 h (5.7 years) to about 300 000 h (34.2 years) for currently available microwave link equipment. The mean time to repair must also be considered in looking at the overall probability of an probability that a single link terminal will fail is

$$terminal\ outage\ probability = 1.0 - \left(\frac{\mathrm{MTBF}}{\mathrm{MTBF} + \mathrm{MTTR}}\right) \tag{15}$$

or 0.00790% for the sample values.

The link fails when the terminal at either end fails, so the link failure probability due to equipment failure is 0.0159% or a link availability of 99.984%. For a link with a high fade margin, the equipment outage probability can dominate the overall link availability.

A link that has a single terminal radio is often referred to as unprotected because of equipment failure may not be acceptable when considering the availability requirements. For this reason, systems intended for high reliability applications usually employ redundant equipment at each terminal. Redundant radio equipment is usually referred to as hot standby equipment, indicating that the equipment is turned on and at operating temperature. It may then be immediately and automatically put into service in the event of failure radio units. A rapid switching process between primary and secondary units interrupts the signal for 20 to 50 ms.

With a hot standby terminal, for the example with the numbers used above, the link availability is 99.99999984%. This availability is substantially higher than can be expected from multipath and rain fade outages, removing equipment failure as a significant factor in determining overall link availability.

Human intervention during maintenance activities can also cause unavailability. The contribution of these factors is generally difficult to predict through mathematical analysis. However, they should be considered when designing radio-relay systems.

At the National Institute of Telecommunications "TrasaZ" computer program has been worked out. This is a radio frequency propagation computer program for the transmission path between an RF transmitter and a receiver. This program compute fades expected from multipath and rain. Earth curvature for standard or substandard atmosphere is taken into account. The program's frequency range is from 1 GHz to 60 GHz.

References

[1] R. H. Anderson, *Fixed Broadband Wireless System Design*. Chichester: Wiley, 2003.

[2] J. Bogucki and E. Wielowieyska, "Propagation reliability of line-of-sight radio-relay systems above 10 GHz", in *17th Int. Wrocław Symp. Exhib. Electromagn. Compatib.*, Wrocław, Poland, 2004, pp. 37–40.

[3] J. Bogucki, A. Dusiński, and E. Wielowieyska, "Problemy propagacyjne w środkach przekazu radiowego. Etap 2: Opracowanie oprogramowania dla potrzeb projektowania horyzontowych linii radiowych pracujących na częstotliwościach zakresu fal milimetrowych". Warszawa: Instytut Łączności, 2004 (in Polish).

[4] J. Bogucki, "Propagacja na trasach horyzontowych (część I)", *Infotel*, no. 7-8, pp. 54–56, 2001 (in Polish).

[5] J. Bogucki, "Propagacja na trasach horyzontowych (część II)", *Infotel*, no. 10, pp. 34–37, 2001 (in Polish).

[6] J. Bogucki, "Zjawisko wielodrogowości w horyzontowych liniach radiowych", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, no. 4, pp. 320–325, 2000 (in Polish).

[7] J. Bogucki, "Próba badań propagacji w pasmie Q", *Prace IŁ*, no. 100, pp. 13–25, 1992 (in Polish).

[8] J. Bogucki, "Wpływ warunków propagacji na niezawodność pracy horyzontowych linii radiowych", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, no. 3, pp. 159–164, 1997 (in Polish).

[9] J. Bogucki and E. Wielowieyska, "Niezawodność horyzontowych linii radiowych – aspekt praktyczny", in *Krajowa Konferencja Radiokomunikacji, Radiofonii i Telewizji KKRRiT*, Wrocław, Poland, 2003, pp. 121–124 (in Polish).

[10] R. K. Crane, *Propagation Handbook for Wireless Communications System Design*. London: CRC Press, 2003.

[11] M. P. M. Hall, *Effects of Troposphere on Radio Communication*. London: Peter Peregrinus, 1979.

[12] "Propagation data and prediction methods required for the design of terrestrial line-of-sight systems", ITU-R Rec. P.530-11, 03-2005.

[13] "Specific attenuation model for rain for use in prediction methods", ITU-R Rec. P.838-3, 03-2005.

[14] "Computation of reliability and compatibility of HF radio systems", ITU-R Rec. P.842-3, 03-2005.

[15] "Availability objective for radio-relay systems over a hypothetical reference circuit and a hypothetical reference digital path", ITU-R Rec. F.557-4, 09-1997.

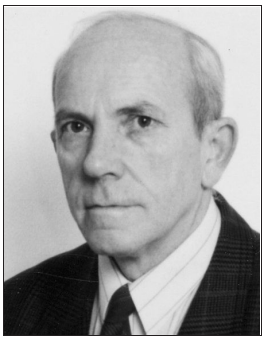
[16] A. Kawecki, "Charakterystyki zaników sygnału wywołanych propagacją wielodrogową w doświadczalnych liniach radiowych 11,5 GHz i 18,6 GHz", *Prace IŁ*, no. 101, pp. 59–83, 1993 (in Polish).

[17] A. Kawecki, "Some aspects of attenuation due to rain prediction and rain rate correlation with attenuation", *Prace IŁ*, no. 104, pp. 67–93, 1995.

[18] A. Kawecki, "Wieloletnie charakterystyki intensywności deszczu w Miedzeszynie na potrzeby radiokomunikacji", *Prace IŁ*, no. 106, pp. 69–84, 1996 (in Polish).

[19] C. Salema, *Microwave Radio Links: From Theory to Design*. New Jersey: Wiley, 2003.

[20] A. A. R. Townsend, *Digital Line-of-Sight Radio Links. A Handbook*. London: Prentice Hall, 1988.



Jan Bogucki was born in 1947 in Warsaw, Poland. He graduated from Technical University of Warsaw (1972). Since 1973 he has been employed at National Institute of Telecommunications (NIT), Warsaw, where he has been engaged in problems connected with digital radio links, digital television, microwave propagation in the troposphere and electromagnetic compatibility. He is the author or co-author of over 100 publications in scientific journals and conference proceedings.
e-mail: J.Bogucki@itl.waw.pl
National Institute of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

Ewa Wielowieyska was born in 1952 in Warsaw, Poland. She graduated from Faculty of Mathematics, Informatics and Mechanics of Warsaw University. Since 1981 she has been employed at National Institute of Telecommunications (NIT), Warsaw, where she has been engaged in tasks connected with software of measurement systems and problems of microwaves propagation in the troposphere, propagation of digital radio signals on short and medium waves.
e-mail: E.Wielowieyska@itl.waw.pl
National Institute of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

Information for authors

Journal of Telecommunications and Information Technology **(JTIT)** is published quarterly. It comprises original contributions, both regular papers and letters, dealing with a wide range of topics related to telecommunications and information technology. **All regular papers and letters are subject to peer review**. Topics presented in the JTIT report primary and/or experimental research results, which advance the base of scientific and technological knowledge about telecommunications and information technology.

The JTIT is dedicated to publishing research results which advance the level of current research or add to the understanding of problems related to modulation and signal design, wireless communications, optical communications and photonic systems, voice communications devices, image and signal processing, transmission systems, network architecture, coding and communication theory, as well as information technology.

Suitable research-related papers should hold the potential to advance the technological base of telecommunications and information technology. Tutorial and review papers are published only by invitation.

Manuscript. Papers published by invitation and regular papers should contain up to 15 and 8 printed pages respectively (one printed page corresponds approximately to 3 double-spaced pages of manuscript where one page contains approximately 2000 characters). An original and one copy of the manuscript should be submitted, each completed with all illustrations, tables and figure captions attached at the end of the paper. Tables and figures should be numbered consecutively with Arabic numerals. The manuscript should include an abstract about 100 words long and the relevant keywords. The abstract should contain statement of the problem, assumptions and methodology, results and conclusion or discussion on the importance of the results.
The manuscript should be double-spaced on one side of each A4 sheet (210 × 297 mm) only. Use of computer notation such as Fortran, Matlab, Mathematica, etc., for formulae, indices and the like is not acceptable and will result in automatic rejection of the manuscript.

Illustrations. Original illustrations should be submitted. Drawings in Corel Draw and Postscript formats are preferred. Colour illustrations are accepted only under exceptional circumstances. Lettering should be large enough to be readily legible when drawing is reduced to two- or one-column width, which often means shrinking to 1/4th of original size. Photographs should be used sparingly. All photographs should be delivered in electronic formats (TIFF, JPG, PNG or BMP). Page numbers including tables and illustrations (which should be grouped at the end) should be put in a single series, with no numbers skipped.

References. All references should be marked in the text by Arabic numerals in square brackets and listed at the end of the paper in order of their appearance in the text, including exclusively publications cited inside. Samples of correct formats for various types of references are presented below:

[1] Y. Namihira, "Relationship between nonlinear effective area and mode field diameter for dispersion shifted fibres", *Electron. Lett.*, vol. 30, no. 3, pp. 262–264, 1994.

[2] C. Kittel, *Introduction to Solid State Physics*. New York: Wiley, 1986.

[3] S. Demri and E. Orłowska,"Informational representability: Abstract models versus concrete models", in *Fuzzy Sets, Logics and Knowledge-Based Reasoning*, D. Dubois and H. Prade, Eds. Dordrecht: Kluwer, 1999, pp. 301–314.

Biographies and photographs of authors. A brief professional author's biography of up to 100 words and a photo of each author should be included with the manuscript. A printed photo, minimum size 35 × 45 mm, is acceptable. The photo may be supplied as image file.

Electronic form. TEX and LATEX are preferable, standard Microsoft Word format (.doc) is acceptable. The JTIT LATEX style file is available to authors. The file(s) should be submitted by e-mail or on a floppy disk or CD together with the hard copy of the manuscript. It is important to ensure that the diskette version and the printed version are identical. The diskette should be labelled with the following information: a) the operating system and word processing software used; b) in case of UNIX media, the method of extraction (i.e., tar) applied; c) file name(s) related to manuscript. The diskette or CD should be properly packed in order to avoid possible damage in the mail.

Galley proofs. Authors should return proofs as soon as possible. In other cases, the article will be proof-read against manuscript by the editor and printed without the author's corrections. Remarks to the errata should be provided within two weeks after receiving the offprint.

Copyright. Manuscript submitted to JTIT should not be published or simultaneously submitted for publication elsewhere. By submitting a manuscript, the author(s) agree to automatically transfer the copyright for their article to the publisher, if and when the article is accepted for publication. The copyright comprises the exclusive rights to reproduce and distribute the article, including reprints and all translation rights. No part of the present JTIT should not be reproduced in any form nor transmitted or translated into a machine language without prior written consent of the publisher.

A copy of the JTIT is provided to each author of paper published.
