Optimal Duration Five Bit Orthogonal Chaotic Vector Shift Keying Communication: A Case Study

Timothy J. Wren, *Member, IEEE*
School of Engineering & Design, University of Sussex, Brighton, East Sussex, England, BN1 9RH
T.J.Wren@sussex.ac.uk

Tai C. Yang
School of Engineering & Design, University of Sussex, Brighton, East Sussex, England, BN1 9RH
T.C.Yang@sussex.ac.uk

***Abstract*—This paper presents a case study of three different five bit multidimensional constellations using Orthogonal Chaotic Vector Shift Keying (OCVSK); a two dimensional chaotic QPSK equivalent scheme (QCSK), a spherical Triakis Icosahedral scheme and a five dimensional hypercubic constellation. The optimal duration for each signal chip within the scheme is determined, in the light of the perceived noise within the channel, and the results are presented. The conclusion drawn is that the higher the dimension of the scheme and the consequential simplicity of the structure, the greater the noise rejection.**

Keywords-component; orthogonal chaotic vector shift keying; Gram-Schmidt orthonormalization process

I. INTRODUCTION

Since the introduction of Orthogonal Chaotic Vector Shift Keying (OCVSK) by Wren *et al.* [1-3] research has continued into its noise rejection properties. Presented is a case study of three examples of OCVSK, all using five bit schemes giving thirty two different messages, and demonstrating the improvements afforded by an increase in the dimensionality of the transmission schemes. OCVSK extends both the regions of interest of Kolumbán *et al* [7-11]; where the concepts of BPSK were extended to use chaotic signals, and Galias and Maggio [4] who introduced the concept of orthogonal chaotic signals within a Quadrature Chaotic Shift Keying (QCSK) scheme. Neither of these research areas extended the concept of chaotic signal orthogonality beyond two dimensions. In order to increase the data rate of these schemes symbolic constellations need to be introduced which are comparable to Quadrature Amplitude Modulation (QAM) and the like. If, for reasons of secure communication for example, the power of the signals needs to be invariant, then only schemes that have constellation symbols on circular constellations are valid. This introduces a problem of inter-symbolic separation and a consequential problem with noise rejection. By introducing more dimensionality the inter-symbolic separation can be increased and the noise rejection greatly improved.

978-1-61284-671-2/11/$26.00 ©2011 IEEE

In this case study three different five bit multidimensional constellations using OCVSK are highlighted. A two dimensional chaotic QCSK scheme, a three dimensional spherical Triakis Icosahedral scheme and a five dimensional hypercubic constellation. Transmission simulations have been carried out and Bit Error Rate (BER) simulations have been determined using a novel method introduced by Wren *et al.* [1-3] and described in section II *B*.

In addition, section II *C* describes a new optimal duration signal length method. This is determined from the perceived noise within the channel and the potential information content of the scheme.

A brief theoretical background of the ideas within OCVSK is given in section II and a description of the scheme constellations within this case study are described in section III. The transmission simulation and BER results are presented in section IV and conclusions drawn in section V.

II. THEORY

A. Orthogonal Chaotic Vector Shift Keying

Consider a system, with an m dimensional constellation, that relies on m different mutually orthogonal signals, which actually form part of an orthonormal basis of functions $u_i(t)\ \forall\ i \in [1,m]$. As with a QPSK scheme a message can be encoded using these orthogonal functions by combining them linearly using encoding coefficients. This can now be represented as

$$s(t) = c_1 u_1(t) + c_2 u_2(t) + c_3 u_3(t) + \ldots + c_m u_m(t) \quad (1)$$

which in vector function notation becomes

$$s(t) = \mathbf{u}^T(t)\mathbf{c} \quad (2)$$

where

$$\mathbf{u}^T(t) = [u_1(t), u_2(t), u_3(t), \ldots, u_m(t)] \quad (3)$$

and

$$\mathbf{c}^T = [c_1, c_2, ..., c_m] \quad (4)$$

this is the message signal for each symbol in the message.

At the receiver the symbols can be retrieved by determining the coefficients of individual orthogonal components by using the m correlation integrals

$$c_i = \frac{1}{P_i T}\int_0^T s(t)u_i(t)dt \quad \forall \quad i \in [1,m] \quad (5)$$

$$P_i = \frac{1}{T}\int_0^T u_i^2(t)dt \quad (6)$$

or from equations 2-6

$$\int_0^T \mathbf{u}(t)s(t)dt = \int_0^T \mathbf{u}(t)\mathbf{u}^T(t)\mathbf{c}dt \quad (7)$$

Therefore this can be written in concise vector notation as

$$\mathbf{c} = \left[\int_0^T \mathbf{u}(t)\mathbf{u}^T(t)dt\right]^{-1}\int_0^T \mathbf{u}(t)s(t)dt \quad (8)$$

This will work with any set of signals if they are independent. If there is no noise present, the signal sets are orthogonal and the inversion is simplified by the matrix being diagonal. However in the presence of noise, the inversion can influence the noise rejection characteristics of decoding. Noise rejection can be improved by discarding non diagonal terms because they are perceived to have been generated by noise. The scheme of signal transmission here is irrelevant to the above derivation. The signals can be transmitted simultaneously on multiple channels or contiguously on one channel.

A discrete version of these equations is required for use within a Software Defined Radio (SDR). Consider the n signal vector $\mathbf{x}$ produced by taking n samples of a chaotic process. Each sampled vector has the mean value removed thus leaving it as samples of a zero mean process. An $n \times m$ matrix $\mathbf{X}$ is formed from collections of n length $\mathbf{x}$ vectors. Each $\mathbf{x}$ vector of these collections remains persistent within the encoding architecture over m symbolic transmissions. Each symbol sequence transmits m bits of information so the transmission efficiency of this scheme is high, because the symbolic and bit data rate is only dependent on the length of each signal vector. Now an $n \times m$ orthonormal matrix $\mathbf{U}$ is generated from the $\mathbf{X}$ matrix using the Gram-Schmidt process. The matrix $\mathbf{U}$ is multiplied by a diagonal power balancing matrix $\mathbf{P}$ to produce a matrix $\mathbf{Q}$ as

$$\mathbf{Q} = \mathbf{UP} \quad (9)$$

The choice of the diagonal matrix $\mathbf{P}$ is arbitrary but specifying it in terms of a signal to noise power ratio will become significant in section *B*. The same diagonal value of the $\mathbf{P}$ matrix is used to power balance the most recent normalized $\mathbf{x}$ vector before it is transmitted as the $\mathbf{z}$ vector. That is

$$\mathbf{z} = \tilde{\mathbf{x}}p \quad (10)$$

where $\tilde{\mathbf{x}}$ here is the normalized form of $\mathbf{x}$ that is

$$\tilde{\mathbf{x}}^T\tilde{\mathbf{x}} = 1 \quad (11)$$

A new $\mathbf{X}$ matrix is created after each $\mathbf{x}$ vector is sampled as

$$\mathbf{X}_{n,m} = [\mathbf{x} \quad \mathbf{X}_{n,m-1}] \quad (12)$$

It is now necessary only to encode a single symbol after each n samples represented by an $\mathbf{s}$ vector as

$$\mathbf{s} = \mathbf{Qc} \quad (13)$$

and this is transmitted in that same way as the $\mathbf{z}$ vector.

Consider now the method for decoding each received signal vector; this is the equivalent of the correlation integral in equation 8 and is a least squares approximation of the encoding vector given a noisy received signal vector $\bar{\mathbf{s}}$. If the received signal is considered then

$$\bar{\mathbf{s}} = \mathbf{Qc} + \sigma\boldsymbol{\varepsilon} \quad (14)$$

the noise term contains $\boldsymbol{\varepsilon}$ which is Gaussian White noise process with a zero mean and a unit variance, that is $E\{\boldsymbol{\varepsilon}_i\} = \mathbf{0}$ and $E\{\boldsymbol{\varepsilon}_i^T\boldsymbol{\varepsilon}_i\} = n$. In the following equations, the $\bar{\ }$ notation indicates a variable derived from received signal data and the ^ indicates an estimated value. Now the signal estimate for a particular symbol represented by a received signal vector $\bar{\mathbf{s}}$ is given by

$$\hat{\mathbf{s}} = \overline{\mathbf{Q}}\hat{\mathbf{c}} \quad (15)$$

expressing the error between the received signal vector and the estimated one as

$$\mathbf{e} = \bar{\mathbf{s}} - \hat{\mathbf{s}} \quad (16)$$

and forming a squared error sum as

$$\eta = \mathbf{e}^T\mathbf{e} \quad (17)$$

now minimize η with respect to the estimate of the encoding vector $\hat{\mathbf{c}}$ so

$$2\mathbf{e}^T\frac{\partial\mathbf{e}}{\partial\hat{\mathbf{c}}} = \mathbf{0}^T \quad (18)$$

from equations 15 and 16

$$\frac{\partial\mathbf{e}_i}{\partial\hat{\mathbf{c}}_i} = -\overline{\mathbf{Q}} \quad (19)$$

Therefore equation 18 can be rearranged, incorporating equations 15 and 16 as

$$\overline{\mathbf{Q}}^T(\overline{\mathbf{s}}-\overline{\mathbf{Q}}\hat{\mathbf{c}})=\mathbf{0} \tag{20}$$

And finally forming an estimate of the encoding vector by rearranging equation 20 as

$$\hat{\mathbf{c}}=\left[\overline{\mathbf{Q}}^T\overline{\mathbf{Q}}\right]^{-1}\overline{\mathbf{Q}}^T\overline{\mathbf{s}} \tag{21}$$

The $\overline{\mathbf{Q}}$ matrix needs to be estimated from the persistent received reference matrix $\overline{\mathbf{Z}}$ created as

$$\overline{\mathbf{Z}}_{n,m}=[\overline{\mathbf{z}} \quad \overline{\mathbf{Z}}_{n,m-1}] \tag{22}$$

now both $\overline{\mathbf{U}}$ and $\overline{\mathbf{Q}}$ matrices can be formed by using the $\overline{\mathbf{Z}}$ matrix via the Gram-Schmidt process. The decoding equation 21 can now be simplified by substituting the received form of equation 9 into equation 21 to give

$$\hat{\mathbf{c}}=\mathbf{P}^{-1}\overline{\mathbf{U}}^T\overline{\mathbf{s}} \tag{23}$$

where

$$\mathbf{P}^{-1}=\frac{1}{p}\mathbf{I}_m \tag{24}$$

where p is the power balancing gain.

This scheme has a robust estimating structure because it avoids the noise transmission through an m dimensional matrix inversion and it has the same dependency on the nature of the noise transmission through the Gram-Schmidt process. The cyclic transmission efficiency is increased and is scalable with the dimension m, without any noise or time penalties.

B. *Signal Characterization*

The symbol encoding vector estimate can be expressed as follows

$$\hat{\mathbf{c}}=[\overline{\mathbf{Q}}^T\overline{\mathbf{Q}}]^{-1}\overline{\mathbf{Q}}^T\overline{\mathbf{s}} \tag{25}$$

it has been shown by Wren [2] that the estimate can be expressed in terms of the noise on the transmission channel and the original idealized symbol encoding vector by

$$\overline{\mathbf{Q}}=\sigma\sqrt{nP_{snr}}\cdot\mathbf{G}\left(\sqrt{nP_{snr}}\cdot\begin{bmatrix}\mathbf{I}_m\\ \mathbf{0}_{n-m,m}\end{bmatrix}\mathbf{W}+\mathbf{E}\right)$$
$$=\sigma\sqrt{nP_{snr}}\cdot\overline{\mathbf{U}} \tag{26}$$

and

$$\overline{\mathbf{s}}=\sigma\left(\sqrt{nP_{snr}}\cdot\begin{bmatrix}\mathbf{I}_m\\ \mathbf{0}_{n-m,m}\end{bmatrix}\mathbf{c}+\boldsymbol{\varepsilon}\right) \tag{27}$$

which yields

$$\hat{\mathbf{c}}=\left(\left(\sigma\sqrt{nP_{snr}}\cdot\overline{\mathbf{U}}\right)^T\left(\sigma\sqrt{nP_{snr}}\cdot\overline{\mathbf{U}}\right)\right)^{-1}\cdots$$
$$\cdots\sigma\left(\sqrt{nP_{snr}}\cdot\overline{\mathbf{U}}\right)^T\sigma\left(\sqrt{nP_{snr}}\cdot\begin{bmatrix}\mathbf{I}_m\\ \mathbf{0}_{n-m,m}\end{bmatrix}\mathbf{c}+\boldsymbol{\varepsilon}\right)$$
$$=\overline{\mathbf{U}}^T\left(\begin{bmatrix}\mathbf{I}_m\\ \mathbf{0}_{n-m,m}\end{bmatrix}\mathbf{c}+\frac{1}{\sqrt{nP_{snr}}}\boldsymbol{\varepsilon}\right) \tag{28}$$

where

$$\overline{\mathbf{U}}=\mathbf{G}\left(\sqrt{nP_{snr}}\cdot\begin{bmatrix}\mathbf{I}_m\\ \mathbf{0}_{n-m,m}\end{bmatrix}\mathbf{W}+\mathbf{E}\right) \tag{29}$$

The result here is constructed using the power of the signal to noise ratio P_{snr} , whereas most of the literature quotes the equations and results in terms of the 'energy per bit divided by the noise power', that is $\frac{E_b}{N_0}$. This depends on the bit transmission rate, which in turn, is dependent on the structure of the different signal sequences. P_{snr} is independent of transmission structure. If the transmission bit rate B_r is known and the energy is spread over the reference and the signal sequences then

$$\frac{E_b}{N_0}=\frac{P_{snr}}{2\tau B_r} \tag{30}$$

For orthogonal minimal constellations the bit rate, including the reference sequence time is given by

$$B_r=\frac{m}{2n\tau} \tag{31}$$

where τ is the sampling time of the system. Substituting equation 31 into 30 and rearranging gives

$$P_{snr}=\frac{m}{n}\cdot\left(\frac{E_b}{N_0}\right) \tag{32}$$

yielding

$$\hat{\mathbf{c}}=\overline{\mathbf{U}}^T\left(\begin{bmatrix}\mathbf{I}_m\\ \mathbf{0}_{n-m,m}\end{bmatrix}\mathbf{c}+\frac{1}{\sqrt{m\left(\frac{E_b}{N_0}\right)}}\boldsymbol{\varepsilon}\right) \tag{33}$$

C. *Optimal Duration Signals*

The selection of signal length is instrumental in determining the data transmission rate. It has been shown by Wren *et al*. [1-2] that increases in signal length increases noise rejection at the cost a reduction in the data transmission rate. How is an heuristic optimal signal length chosen given certain transmission channel parameters?

For the proposed scheme to work each signal sequence needs to be independent of the last *m* other signal sequences. So consider the independence of the columns of **X** made up from the last *m* sequences, and how this relates to the potential number of bits of precision that the signal set values may be in error. In order to determine if the last signal sequence is 'good' enough for transmission, an estimate of the 'bits' in precision error (B_e) can be determined from the matrix 2-norm condition number C_n as

$$B_e \propto \log_2(C_n) \tag{34}$$

where the condition number is given as

$$C_n = \max\left(\sqrt{\lambda_i}\right)/\min\left(\sqrt{\lambda_i}\right) \quad \forall \quad i \in [i, m] \tag{35}$$

here the λ_i represent the eigenvalues of the symmetric matrix $\mathbf{X}^T\mathbf{X}$ and $\sqrt{\lambda_i}$ are the singular values of X. Initially the signal sets are chosen from the chaotic process and normalized to form the **Z** matrix. If by applying equation 34 to the condition of this matrix a B_e of greater than 1 is obtained then the vector length is doubled and the process repeated. On subsequent derivations of the **z** vector, at each symbol transmission, the B_e must be smaller than 1 and the power of the new chaotic sequence must be greater than a prescribed limit. This optimal method ensures that the signal contains sufficient information and is capable of rejecting the perceived noise within the channel.

III. Transmission Schemes

A. Five Bit Signal Constellations

1) Quadrature Chaotic Shift Keying

The QCSK constellation can be represented in the complex plane as equi-spaced symbolic points on a unit circle, figure 1. The inter-symbolic separation is given as

$$d = 2\sin\left(\frac{\pi}{2^m}\right) \tag{36}$$

which for *m*=5 gives 0.19603 of the radius.

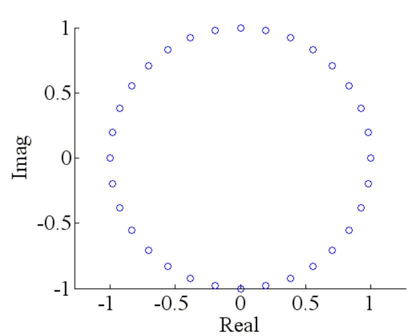

Figure 1: QCSK Constellation

2) Triakis Icosahedral Constellation

A Triakis Icosahedron is the first stellated form of an icosahedron. The twelve vertices of the original polyhedron are supplemented by the addition of triangular based pyramids on each of the twenty faces thus giving a total of thirty two vertices as shown in figure 2. This is not a regular convex polyhedron but a stellated form with all of the vertices made to lie on a unit 3-sphere giving a minimum separation of 0.6409 of the radius.

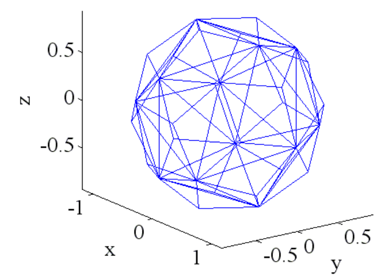

Figure 2: Triakis Icosahedral Constellation

3) Five Dimensional Hypercubic Constellation

The five dimensional constellation takes the form of a fifth order hypercubic 5-polytope. It is a dimensionally extended two dimensional QCSK two bit four symbol constellation. The inter-symbolic separation is given as

$$d = \frac{2}{\sqrt{m}} \tag{37}$$

which for *m*=5 gives 0.89443 of the radius.

Constellation	Dimension (*m*)	Inter-Symbol Separation
QCSK	2	0.19603
Triakis Icosahedron	3	0.64085
Hypercubic 5-Polytope	5	0.89443

Table 1: Inter-Symbolic Separation

B. Generalized Chaotic Transmission System Architecture

A generalized system architecture has been developed to test any dimensional scheme of the form presented in this case study, see figure 3.

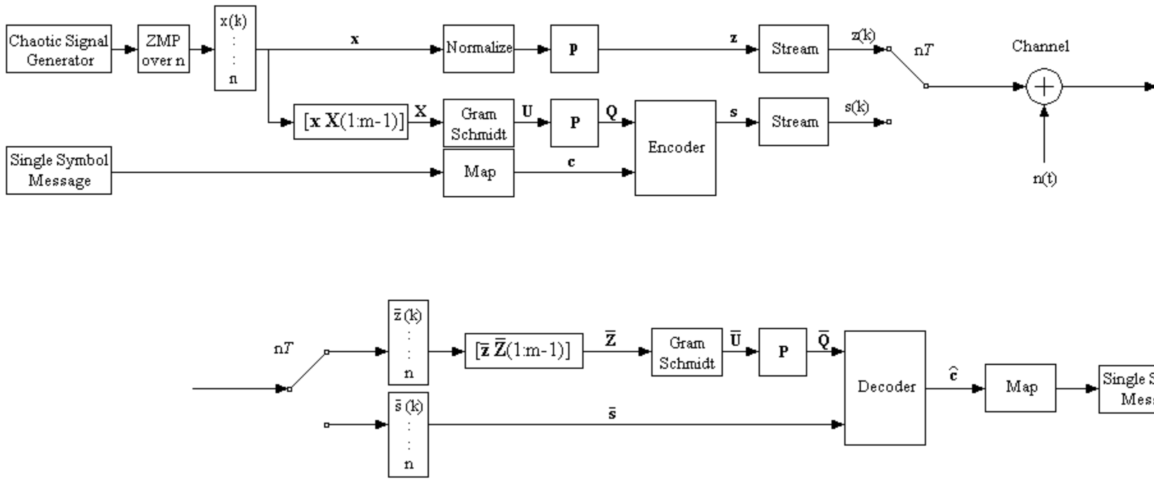

Figure 3: Generalized Chaotic Transmission System Architecture

IV. Simulations

A. Transmission Simulations

Figure 4 illustrates the results of simulating the hypercubic 5-polytope scheme with a signal to noise ratio of $P_{snr} = 1.0$. Graph (a) shows a single vector sequence **x,** and graph (b) shows the persistent matrix **X** of zero mean sampled sequences, generated from the chaotic process. Graph (c) shows the orthonormal basis matrix sequences **U**, generated from the matrix **X** which in turn, when multiplied by the diagonal power balancing matrix **P**, give rise to the **Q** matrix which is used for encoding the signals sequence vector **s**. In this scheme, the references are generated from the **x** vector by normalizing and power balancing it with the power value *p,* to generate the streamed and transmitted **z** vector. When these sequences are resampled at the receiver, they have been contaminated by noise, and assembled into a persistent $\overline{\mathbf{Z}}$ matrix as shown in graph (d).

The same set of transmitted and received 'five' bit messages are shown in figure 5 graphs (a) and (b). Graph (c) demonstrates that there are no errors between the transmitted and the received message sequence, when the time delay is accounted for. The first *m* signals are always in error as the persistent matrices are not fully populated until five message sequences have been transmitted. Graph (d) shows the comparison of the optimal and original condition of the **Z** matrix at each symbol transmission.

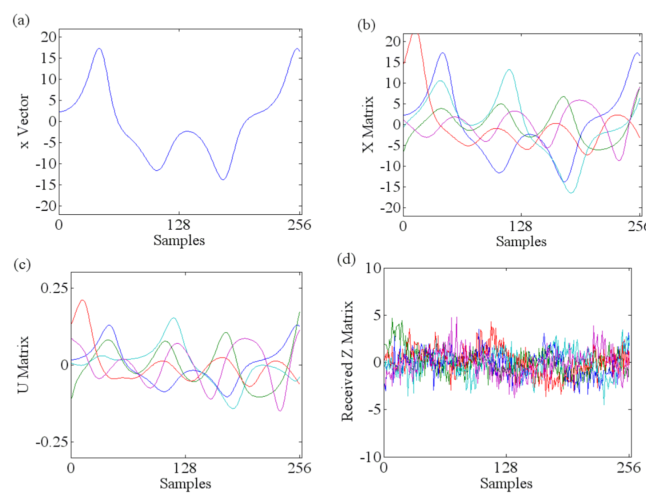

Figure 4: OCVSK 32 Message Transmissions.
$n = 256$, $m = 5$ and Power of Signal to Noise Ratio = 1.0
(a) Transmitter zero mean chaotic sequences **x**
(b) Persistent chaotic sequences **X**
(c) Generated orthogonal reference sequences **U**
(d) Received power balanced reference sequences $\overline{\mathbf{Z}}$

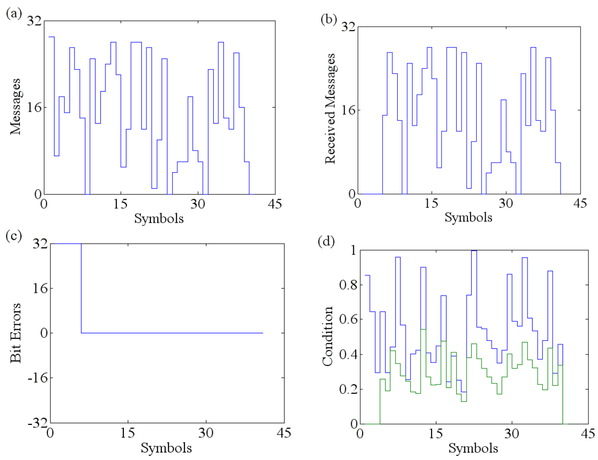

Figure 5: OCVSK 32 Message Transmissions.
$n = 256$, $m = 5$ and Power of Signal to Noise Ratio = 1.0
(a) Transmitted 5 bit message for encoding
(b) Received decoded 5 bit message
(c) Transmitted/Received 5 bit message delayed error
(d) Original versus Optimal conditioning

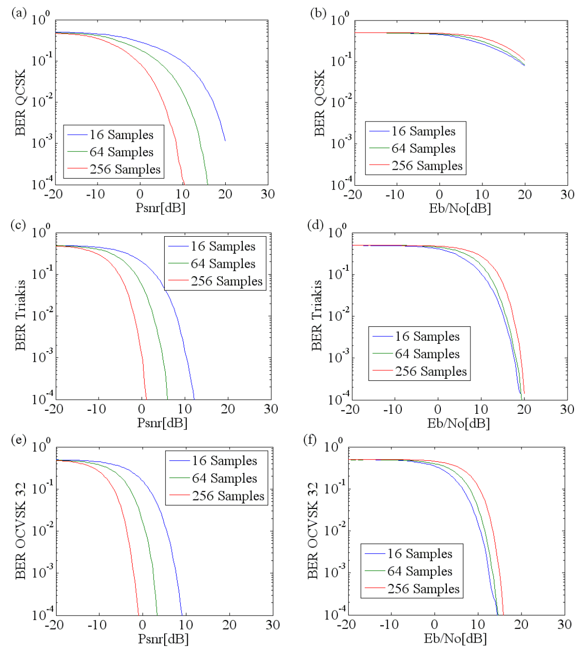

Figure 6: Direct '*m*' Symbol 'U' Scheme. BER v P_{snr} and $\frac{E_b}{N_0}$ Comparison Plot for $n \in [16,64,256]$ samples

(a) and (b) QCSK : BER versus P_{snr} and $\frac{E_b}{N_0}$

(c) and (d) QCSK 32 Symbol Constellation: BER versus P_{snr} and $\frac{E_b}{N_0}$

(e) and (f) OCVSK 32 : BER versus P_{snr} and $\frac{E_b}{N_0}$

B. BER Simulations

Figure 6 shows BER graphs for the three schemes in the case study all with a P_{snr} of 1.0 The QCSK BER of figures 6a and 6b shows worse rates than the Triakis BER example of figures 6c and 6d. The OCVSK 32 example in figures 6e and 6f clearly outperforms the other schemes. The generalized data rate for any orthogonal scheme is $\frac{m}{2n\tau}$, where m is the scheme dimension, n is the number of samples in the chip and τ is the sample time. Clearly as m approaches n the data rate tends towards the Shannon capacity [12]. However, as m increases the BER steadily degenerates so the maximum channel capacity is not realizable. An optimum value for m has been conjectured in [2] for schemes of constant radius which has been found to be a value of m=7.

V. Conclusions

By optimally choosing the signal length of the scheme before transmission the noise rejection properties of the scheme under investigation are increased. This process can be done off line before transmission and the information transmitted to the receiver in the communication preamble and synchronization sequences.

With respect to robustness the conclusion may be drawn that the structure of the OCVSK schemes improves the noise rejection because the effective 'inter-symbolic distances' have been increased by considering a multi-dimensional paradigm rather than an increasingly complex two-dimensional one.

References

[1] T. J. Wren and T. C. Yang, "Orthogonal Chaotic Vector Shift Keying in Digital Communications," IET Communications, vol. IV, Apr., 2010, pp. 739-753.

[2] T. J. Wren, "Orthogonal Chaotic Vector Shift Keying in Digital Communications,", DPhil Thesis, University of Sussex, Oct., 2007

[3] T. J. Wren and T. C. Yang, "On an Improved Chaotic Shift Keying Communication Scheme," International Control Conference (ICC2006), University of Strathclyde, Paper 29, Aug., 2006

[4] Z. Galias and G. M. Maggio, "Quadrature Chaos-Shift Keying," IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications, Vol. 48, Issue 12, 2001, pp. 1510-1519

[5] A. Abel, W. Schwarz and M. Gotz, "Noise Performance of Chaotic Communication Systems," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 47, Issue 12, 2003, pp. 1726-1732

[6] I. Hen and N. Merhav, "On the Threshold Effect in the Estimation of Chaotic Sequences," IEEE Transactions on Information Theory, Vol. 50, Issue 11, 2003, pp. 2894-2904

[7] G. Kolumbán, "Theoretical Noise Performance of Correlator-Based Chaotic Communications Schemes," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 47, Issue 12, 2003, pp. 1692-1701

[8] M. P. Kennedy, N. G. Kolumba, G. Kis and A. Jako, “Recent Advances in Communication with Chaos,” Proc. IEEE Int. Symp. On Circuits and Systems ISCAS’98, 1998, pp. 461-464

[9] N. G. Kolumba, M. P. Kennedy and L. O. Chua, “The Role of Synchronization in Digital Communication Using Chaos – Part I: Fundamentals of Digital Communication,” IEEE Trans. Circuits Syst. I, Issue 44, 1997, pp. 927–935

[10] N. G. Kolumba, M. P. Kennedy and L. O. Chua, “The Role of Synchronization in Digital Communication Using Chaos – Part II: Chaotic Modulation and Chaotic Synchronization,” IEEE Trans. Circuits Syst. I, Issue 45, 1998, pp. 1129–1140

[11] N. G. Kolumba, M. P. Kennedy and G. Kis, “Multilevel Differential Chaos Shift Keying,” Proc. Int. Workshop, Nonlinear Dynamics of Electronics Systems, NDES’97, 1997, pp. 191–196

[12] J. Dunlop, D. Smith, “Telecommunications engineering,” Van Nostrand Reinhold (UK) Co. Ltd., 1984