photon-induced start pulse, the time interval was terminated by the first following pulse derived from the electrical drive to the laser. Fig. 2 shows a typical distribution of start pulse to stop pulse time intervals plotted as a function of time. The three temporal windows in which the photo-counts occur are separated by 1·1 ns as expected, and only the amplitude of the central peak varied when the phase shift in the interferometer was adjusted. Consequently, the system had sufficient time resolution to discriminate between interfering and noninterfering events. The amplitude of the single-photon interference fringes was investigated by scanning the PZT position point by point and integrating the number of photo-counts occurring in the central peak. In addition, at each position the dark count background was estimated from data lying outside the photo-count time window and subtracted from the total count.

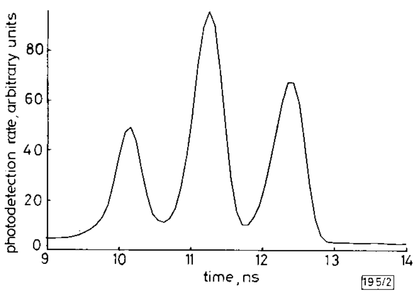

Fig. 2 *Time-interval distribution between single-photon detection start pulses and (first following) laser drive pulses*

A typical series of experiments was preceded by the adjustment of two fibre-polarisation controllers in the interferometer (not shown in Fig. 1 for clarity), in order to match the polarisation states of the interfering pulses. Singe photon data were then acquired as a function of PZT drive voltage. For each PZT voltage, the number of counts in the central peak was normalised to the number of counts obtained from the noninterfering pulses, and the dark count background was subtracted. Fig. 3 shows a typical single photon fringe pattern obtained in this way. A fringe visibility of 91% was calculated from the observed maxima and minima, and the solid line shows a cosinusoidal fit to the data using this value. There are indications of a variation in periodicity in the data, and this probably arises from small amounts of drift in the relative path lengths in the interferometer due to environmental fluctuations which occur during the data acquisition time. The fringe visibility obtained without background subtraction was still relatively high at 78%, indicating that the dark count fraction was relatively small. At the fringe maxima, the number of photo-counts occurring in the central peak corresponded to an average count rate of ~20 kHz. Some experiments were also performed with a lower value of laser

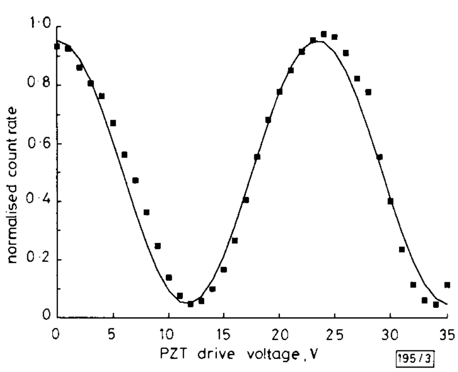

Fig. 3 *Normalised single-photon count rate as function of PZT drive voltage (proportional to phase shift) showing interference fringes with 91% visibility*

attenuation such that the average number of photons per pulse was increased by a factor of 5 to $\mu \simeq 0{\cdot}5$. In this case, the ratio of the photo-count to dark count rate was increased and it was possible to make a more accurate adjustment of the polarisation controllers in the system. This procedure led to higher fringe visibility values of 88 and 93% before and after background subtraction, respectively.

Conclusion: In summary, we have demonstrated a prototype single photon channel that has the potential to form the basis of a future quantum cryptographic system. Relatively high single-photon count rates of ~20 kHz were obtained in the experiment, suggesting that data rates of this order are potentially achievable in a system based on the current design. We note that because the objective of a quantum cryptographic channel is to establish a relatively short secret key (perhaps a few hundred bits), rather than the transmission of the encrypted data itself, a data rate of order 20 kbit/s may be more than adequate.

3rd March 1993

P. D. Townsend (*BT Laboratories, Martlesham Heath, Ipswich, Suffolk IP5 7RE, United Kingdom*)

J. G. Rarity and P. R. Tapster (*DRA Malvern, St Andrews Road, Malvern, Worcestershire WR14 3PS, United Kingdom*)

References

1 BENNETT, C. H., BESSETTE, F., BRASSARD, G., SALVAIL, L., and SMOLIN, J.: 'Experimental quantum cryptography', *J. Cryptology*, 1992, **5**, pp. 3–28

2 BENNETT, C. H., BRASSARD, G., BREIDBART, S., and WEISNER, S.: 'Quantum cryptography or unforgeable subway tokens', *in* CHAUM, D., RIVEST, R. L., and SHERMAN, A. T. (Eds.): 'Advances in cryptology: Proceedings of Crypto '82' (Plenum Press, New York, 1983), pp. 267–275

3 WEISNER, S.: 'Conjugate coding', *SIGACT News*, 1983, **15**. pp. 78–88

4 EKERT, A. K.: 'Quantum cryptography based on Bell's theorem', *Phys. Rev. Lett.*, 1991, **67**, pp. 661–663

5 BENNETT, C. H., BRASSARD, G., and EKERT, A. K.: 'Quantum cryptography', *Sci. Am.*, October 1992, pp. 26–33

6 BENNETT, C. H.: 'Quantum cryptography using any two nonorthogonal states', *Phys. Rev. Lett.*, 1992, **68**, pp. 3121–3124

7 EKERT, A. K., RARITY, J. G., TAPSTER, P. R., and PALMA, G. M.: 'Practical quantum cryptography based on two-photon interferometry', *Phys. Rev. Lett.*, 1992, **69**, pp. 1293–1295

8 BROWN, R. G. W., RARITY, J. G., and RIDLEY, K. D.: 'Characterisation of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching', *Appl. Opt.*, 1986, **25**, pp. 4122–4126

TRELLIS CODED MODULATION SCHEMES FOR SHADOWED RICIAN FADING CHANNELS

C. Tellambura and V. K. Bhargava

Indexing terms: Trellis codes, Modulation, Satellite links

The Canadian mobile satellite (MSAT) channel has been modelled as the sum of lognormal and Rayleigh components to represent foliage attenuation and multipath fading, respectively. The Letter derives a Chernoff based error bound on the performance of trellis coded modulation (TCM) schemes operating on this channel.

Introduction: The Canadian mobile satellite (MSAT) channel has been modelled as the sum of lognormal and Rayleigh components, by which foliage attenuation and multipath fading are represented [1, 2]. As such, it is closely related to a Rician channel. Typically, mobile satellite channels have been modelled as Rician fading channels. The shadowed Rician model appears to be a better representation for the MSAT channel, because the angle of elevation between a mobile user and a geosynchronous satellite is lower in Canada than, for instance, in the United States.

It is recognised that the use of trellis-coded M-ary phase shift keying signalling for mobile satellite communications yields coding gain, improved fade margin, etc. In analysing such schemes, the Chernoff bound is often encountered. For the MSAT channel, however, the Chernoff bound on the pairwise error probability is not available in closed form; numerical integration must be used in its computation. For light and average shadowed Rician fading channels, this Letter provides an approximation that is virtually identical to the exact Chernoff bound. However, the approximation requires significantly less computation. Moreover, it adds insight to the effect of the channel and code parameters that affects the bit error probability. Resulting pairwise error probability resemble those of the Rician channel, and so can be used for evaluating the bit error performance and finding optimal codes for such channels.

System and channel model: We consider a typical system model [3], where binary input data are convolutionally encoded at rate $n/(n+1)$. the encoded $n+1$ bit words are block interleaved and mapped into a sequence $x = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_N)$ of M-ary PSK symbols, which constitute a normalised constellation, i.e. $|x_k|^2 = 1$ for all symbols. For simplicity, we assume ideal interleaving/deinterleaving. The corresponding channel output sequence is [3]

$$y_k = \rho_k x_k + n_k \tag{1}$$

where ρ_k denotes the random fading amplitude, and n_k is a complex Gaussian noise sample with zero mean and variance $(2\bar{E}_s/N_0)^{-1}$. According to the shadowed Rician fading model, each ρ_k is described by the probability density function (PDF) [2]

$$p(\rho_k) = \frac{\rho_k}{b_0\sqrt{(2\pi d_0)}} \int_0^\infty \frac{1}{z} \times \exp -\left[\frac{(\log z - \mu_0)^2}{2d_0} + \frac{\rho_k^2 + z^2}{b_0}\right] I_0\left(\frac{\rho_k z}{b_0}\right) dz \tag{2}$$

for $0 \le \rho_k < \infty$. Here, $z = e^v$; v is Gaussian with mean μ_0 and variance d_0, b_0 is the variance of the multipath component (Rayleigh distributed), $\log(\cdot)$ is the natural logarithm, and $I_0(\cdot)$ is the zero order modified Bessel function. Depending on the degree of shadowing three cases have been identified, and for light shadowing, for example, $b_0 = 0{\cdot}158$, $\mu_0 = 0{\cdot}115$, and $\sqrt{(d_0)} = 0{\cdot}115$ [2].

The PDF in eqn. 2 is difficult to handle mathematically. Hence, to approximate this integral, by substituting $\log z - \mu_0 = t$, it can be converted to Laplace type:

$$p(\rho_k) = \frac{\rho_k}{b_0\sqrt{(2\pi d_0)}} \int_{-\infty}^{\infty} \exp -\left[\frac{\rho_k^2 + e^{2(\mu_0 + t)}}{2b_0}\right] \times I_0\left[\frac{\rho_k e^{(\mu_0 + t)}}{b_0}\right] \exp -\left(\frac{t^2}{2d_0}\right) dt$$

$$\triangleq \int_{-\infty}^{\infty} g(t) \exp -(\gamma t^2)\, dt \tag{3}$$

where $\gamma = 1/(2d_0)$ and $g(t)$ denotes the rest of the integrand in eqn. 3. Because γ is quite large for both light and average cases, this integral can be approximated in terms of $g(0)$, $g''(0)$ and γ. Hence, using the second order Laplace approximation (Reference 4, eqn. 53) for this integral, we have

$$p(\rho_k) = \frac{\rho_k}{b_0}[c_0 \Psi_0(\rho_k) - c_1 \rho_k \Psi_1(\rho_k) + c_2 \rho_k^2 \Psi_0(\rho_k) + c_2 \rho_k^2 \Psi_2(\rho_k)] + O(\gamma^{-5/2}) \tag{4}$$

where

$$\Psi_n(\rho_k) \triangleq \exp -\left(\frac{\rho_k^2 + e^{2\mu_0}}{2b_0}\right) I_n\left(\frac{\rho_k e^{\mu_0}}{b_0}\right) \quad n = 0, 1, 2 \tag{5}$$

in which $c_0 = 1 + 0{\cdot}5d_0(\rho_1^2 - 2\rho_1)$, $c_1 = 0{\cdot}5d_0\rho(2\rho_1 - 1)$, $c_2 = 0{\cdot}25d_0\rho^2$, $\rho = \exp(\mu_0)/b_0$, $\rho_1 = \exp(2\mu_0)/b_0$, and $I_n(\cdot)$ denotes the nth order modified Bessel function.

Pairwise error probability: The pairwise error probability $P(x \to \hat{x})$ is defined to be the probability of choosing the coded sequence $\hat{x} = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_N)$ when in reality $x = (x_1, x_2, \ldots, x_N)$ was transmitted [3], assuming x and $\hat{x}$ are the only choices. Conditional on the set of fading amplitudes $\rho = (\rho_1, \rho_2, \ldots, \rho_n)$, the pairwise error probability is bounded as follows:

$$P(x \to \hat{x} \mid \rho) \le \prod_{k \in \eta} \exp -\left(\frac{\bar{E}_s}{4N_0}\rho_k^2 |x_k - \hat{x}_k|^2\right) \tag{6}$$

where η is the set of indexes k for which $x_k \ne \hat{x}_k$ [3]. Averaging the conditional error bound over each $p(\rho_k)$ in eqn. 4 yields

$$P(x \to \hat{x}) \le \prod_{k \in \eta} \frac{\theta_k}{1 + b_0 \frac{\bar{E}_s}{2N_0}|x_k - \hat{x}_k|^2} \times \exp -\left(\frac{e^{2\mu_0}\frac{\bar{E}_s}{4N_0}|x_k - \hat{x}_k|^2}{1 + b_0\frac{\bar{E}_s}{2N_0}|x_k - \hat{x}_k|^2}\right) \tag{7}$$

where

$$\theta_k \triangleq c_0 - \frac{b_0 d_0 \rho^2(\rho_1 - 1)}{1 + b_0\frac{\bar{E}_s}{2N_0}|x_k - \hat{x}_k|^2} + \frac{0{\cdot}5 d_0 \rho^4}{\left(1 + b_0\frac{\bar{E}_s}{2N_0}|x_k - \hat{x}_k|^2\right)^2} \tag{8}$$

In deriving eqn. 7, we have made use of certain identities involving Bessel functions, and these can be found in Refer-

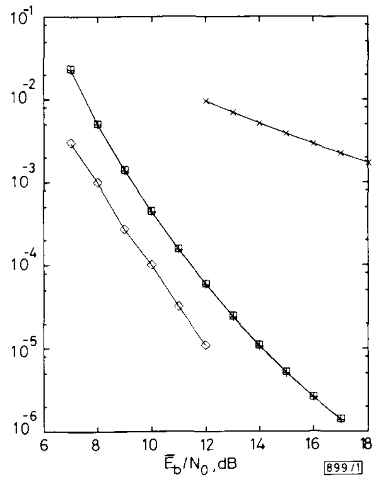

Fig. 1 P_b *against* $\bar{E}_b/N_0$

8-state Trellis code in Reference 6, light shadowed Rician fading, coherent detection

—⊞— TF bound with eqn. 7
—+— TF bound with Chernoff
—◇— simulation
—×— uncoded 4PSK

ence 5. Note that for large signal-to-noise ratios the second and third terms of θ_k tend to zero. This error bound can be readily used with the transfer function of a trellis encoder to find the bit error probability, and adds insight to the effect of the channel and code parameters that affect the overall performance. Thus, eqn. 7 indicates that for the shadowed Rician channel, as for a Rician channel, TCM schemes should be designed to maximise the length of the shortest error event path, and the product of branch distances along that path.

Example: In this study, we use a rate 2/3, eight-state binary convolutional encoder (see Reference 6, Fig. 7) to confirm the accuracy of eqn. 7. The transfer function for this code is given in Reference 6, eqn. 19, and the exact Chernoff bound, computed by integration of eqn. 46, Reference 6 using quadrature techniques, or eqn. 7 can be used with the transfer function bound.

Fig. 1 presents P_b against $\bar{E}_b/N_0$ performance for this code, and we observe that eqn. 7 is virtually indistinguishable from the exact result. As for computational speed, computing eqn. 7 consumes negligible time in comparison to quadrature integration necessary for the exact result. The transfer function bound is within 1 dB of simulation points, confirming the validity of simulation points. Also shown is the performance of equivalent uncoded 4PSK. It is apparent that a significant coding gain is realisable in this case.

Conclusions: A new approximation for the Chernoff bound on the pairwise error probability of TCM schemes operating on the shadowed Rician fading channel has been derived. The approximation gives excellent accuracy and allows for easier bounding of the bit error probability, and so is useful in analysing the coded system performance of channels that are subjected to shadowing.

5th February 1993

C. Tellambura and V. K. Bhargava (*Department of Electrical & Computer Engineering, University of Victoria, PO Box 3055, Victoria BC, V8W 3P6, Canada*)

References

1 LOO, C., MATT, E. E., BUTTERWORTH, J. S., and DUFOUR, M.: 'Measurements and modelling of land-mobile satellite signal statics'. Proc. 1986 vehicular Technology Conf., Texas, May 1986, pp. 262–267

2 LOO, C.: 'A statistical model for a land mobile satellite link', *IEEE Trans.*, 1985, **VT-34**, pp. 122–127

3 DIVSALAR, D., and SIMON, M. K.: 'Trellis-coded modulation for 4800 to 9600 bps transmission over a fading satellite channel', *IEEE J. Sel. Areas Commun.*, 1987, **SAC-5**, pp. 162–175

4 HUANG, J., and CAMPBELL, L.: 'Trellis coded MDPSK in correlated and shadowed Rician fading channels', *IEEE Trans.*, 1991, **VT-40**, pp. 786–797

5 SNEDDON, I. N.: 'Special functions in mathematical physics and chemistry' (Longman, London, 1980), pp. 126–129

6 MCKAY, R. G., MCLANE, P. J., and BIGLIERI, E.: 'Error bounds for trellis-coded MPSK on a fading mobile satellite channel', *IEEE Trans.*, 1991, **COM-39**, pp. 1750–1761

GUIDED QUASISTATIC FIELDS IN ELECTROMAGNETIC MEASUREMENT-WHILE-DRILLING

M. Y. Xia and Z. Y. Chen

Indexing terms: Electromagnetic theory, Guided waves

The quasistatic fields of extremely low frequencies (ELF) employed to communicate from underground to the ground surface in the electromagnetic measurement-while-drilling (EM-MWD) system are investigated. Three types of well, the vertical well, directional well and horizontal well, are considered. Computed results are obtained for various parameters, including the operating frequencies and the Earth's conductivities. It is demonstrated that long drill strings have a guiding effect which is advantageous to the data transmission.

Introduction: In spite of the fact that the electromagnetic measurement-while-drilling (EM-MWD) system has been studied for several decades, it is fair to say that this method is still only in its infancy. It is a real time data transmission system consisting of two parts, the underground part and the surface part. The sophisticated device of the underground part, the crux of the system, acts as a transmitter and is fixed inside the narrow drill string or drill collar. The surface part, acting as a receiver, detects the signals and decodes the quantities that are being measured.

Compared with another system, the so-called mud-pulse method (MPM), the EM-MWD system has three main advantages:

(1) it is a real time system, and does not need drilling to be stopped

(2) it has higher data rates and can measure more varieties of quantities

(3) particularly because of the much greater commercial value of directional and horizontal wells, which are increasingly being drilled in practice, the EM-MWD system is becoming more desirable, as MPM is effective only for vertical wells and cannot be used for these types of well.

The models for the three types of well under consideration are shown in Fig. 1*a–c* (the mud is not shown in the latter two types). The measured quantities, which may include the moment of torsion of the drill string, the underground temperature and pressure, are first transformed into electric signals by different sensors, then the signals are applied to an 'isolation' gap between the drill string and the drill collar and transmitted to the surface by electromagnetic means. They are the E-field excitations. It has been proven that E-field excitation is more efficient than H-field excitation (a ring of magnetic current). The measurement is accomplished by determining the voltage between the upper drill-string and an electrode placed beneath the surface at a distance.

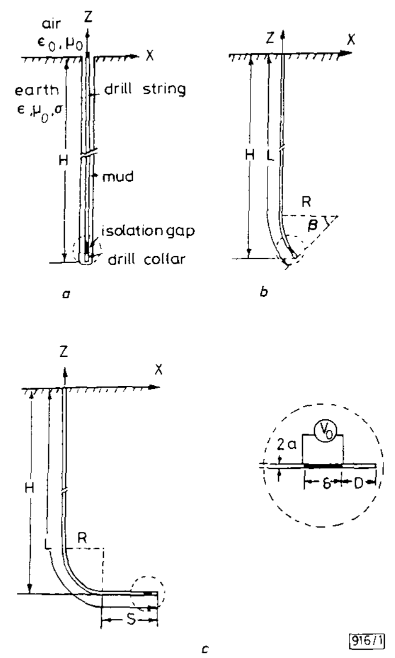

Fig. 1 *Three well models*
a Vertical well
b Directional well
c Horizontal well