Theoretical Model, Simulation Results and Performances of a Secure Chaos-based Multi-user Communication System

Gobindar S. Sandhu and Stevan Berber
(Corresponding author: Gobindar S. Sandhu)

Room 250, 38 Princes Street, Department of Electrical and Computer Engineering
School of Engineering, University of Auckland,Auckland, New Zealand.
(Email: gjumpman@gmail.com)

(Received Dec. 15, 2005; revised and accepted May 2, 2007)

Abstract

Single user chaotic communication system is well known and documented in recent years as a system that enhance the security in signal transmission. In this paper, we propose a multiuser chaos-based communication system. We will present the results of the investigation of this proposed system, called Chaotic Phase Shift Keying, obtained by simulation, operating in white Gaussian noise channel. The theoretical expression for the probability of error is derived and compared to the bit error rate (BER) characteristics of the system obtained by simulation. The results reveal that the simulated system achieves excellent BER performance, matching that of theoretical CPSK.

Keywords: Chaos-based communications, secure communications

1 Introduction

In the past decade, there has been extensive growth and demand in personal communications services. In many cases, users must be provided access to the same or adjacent frequency band simultaneously. However, mobile radio systems are limited by interference from other users [3].

The concept of cryptologia with chaotic systems was introduced by Pecora and Carroll in 1990 [2]. The idea of a chaos shift keying (CSK) system was first proposed by Parlitz et al. [4] and Dedieu et al. [5], and it is to encode digital information using chaotic basis signals. In this system the transmitter consists of two generators, generating two different basis functions. In each bit duration, depending on the transmitted bit (+1 or -1), only one basis function will be used for mapping. The CSK receiver relies on the self-synchronizing properties of chaotic systems, in which the exact replica of the basis signal can be generated at the receiver. The receiver has a correlator, which evaluates the correlation between the basis signal and the received signal, and a decision circuit, which determines what the binary value of the received bit is [11].

In this paper, the theory behind chaotic phase shift keying (CPSK), an idea which was first proposed in 1995 [7] and has been investigated by others since then [10, 12], will be studied. The analytical solution for a multi-user CPSK system, such as the bit error rate formula, and simulation results will be presented and compared with the CSK ones, mentioned in [11]. In particular the aspect of system capacity improvement will also be discussed.

2 Chaotic Transceiver Scheme - Chaotic Phase Shift Keying (CPSK) in AWGN Channel

In past five years, a lot of research effort has been put into the study of digital transceiver schemes using chaotic signals [11, 3, 9, 8, 6]. A single-user chaotic communication system consists of 3 components (See Figure 1). Firstly, it is the transmitter, which includes an encoder, a chaotic signal generator and a chaotic modulator. Secondly, it is the receiver, which has a demodulator and a decoder. Lastly, it is the communication channel, where noise is added onto the modulated signal approaching the receiver. In our analysis, the frequency up conversion will be excluded and a baseband signal analysis will be conducted.

The main difference between the CPSK system that is proposed here and well-known CSK system is that only one chaotic sequence generator exists in each of the transmitter and receiver in the proposed CPSK system. For the CSK system, two sequence generators are required in each of the transmitter and receiver.

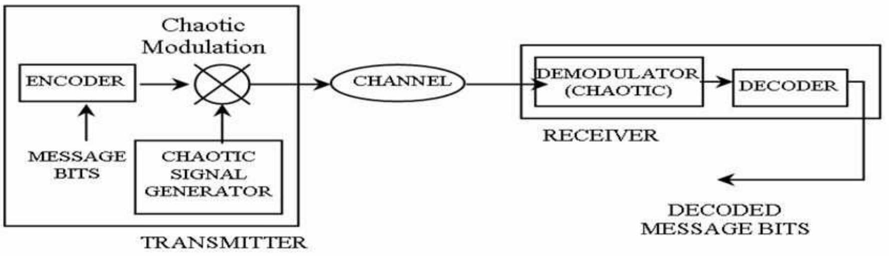

Figure 1: Block diagram of a chaotic communication system

2.1 Theoretical Model of a Chaotic PSK System

Without loss of generality, we will analyze a multi-user communication system, called the baseband communication system shown in Figure 2. The system consists of N transmitters at the base station and N receivers, where each receiver belongs to a single user. Each transmitter consists of a chaotic sequence generator and a modulator. The modulated sequence will be combined with those of the other users, and passed through the channel, where noise (AWGN) is added onto the combined sequence. Each receiver consists of a chaotic sequence generator, for locally generating chaotic sequences, and a correlator and a decision circuit, for estimating the original transmitted sequence.

Let's denote the outputs of the chaotic generators, called the chaotic sequences, by $\{x_t\}$ and the transmitted bits by $\{\gamma_1, \gamma_2, \gamma_3, \ldots\}$. Let $\gamma_i \in (+1, -1)$ be the i^{th} transmitted bit, assuming the probabilities of occurrence of +1 and -1 are equal. Let 2β be the spreading factor, which corresponds to the number of chaotic samples in each transmitted bit. During the i^{th} bit duration, i.e. for discrete time $t = 2\beta(i-1)+1, 2\beta(i-1)+2, \ldots, 2\beta_i$, the transmitter's output of the n^{th} user, $s_t^{(n)}$, is $x_t^{(n)}$ if the transmitted bit is +1. Else if transmitted bit is -1, then transmitter's output will be equal to $-x_t^{(n)}$. The Cubic Map is chosen as the mapping scheme for the chaotic sequence generator, due to its excellent correlation properties [11]. The chaotic samples for each user are generated by different initial conditions. The mean value of each of the N generated chaotic sequences, $E[x_t^{(n)}]$, is zero.

This scheme is called chaotic phase shift keying (CPSK) because only one generator is needed at the transmitter, and if and only if the transmitted bit is -1, there will be an 180o phase shift to the chaotic sequence (i.e. it is multiplied by -1).

The noisy channel distorts the transmitted signal, and the signal at the input of any receiver at time t is given by

$$r_t = \Sigma_{n=1}^{N} s_t^{(n)} + \xi_t,$$

where the first term is the total output of the transmitter at time t, and the second term, ξ_t, is the additive white Gaussian noise, with zero mean and the variance (i.e. power spectral density) equal to $N_0/2$.

At the end of the i^{th} bit duration, the output of the correlator of the n^{th} user is

$$z_i^{(n)} = \Sigma_{t=2\beta(i-1)+1}^{2\beta_i} r_t \cdot x_t^{(n)},$$

which is then compared to the decision value of zero.

2.2 Probability of Error Derivation

The probability of error, as the basic measure of quality of any digital communication system, will be derived in this section for the g^{th} user. For the first symbol (i.e. $i = 1$) sent by the g^{th} user, the correlator output is given by

$$z_1^{(g)} = \sum_{t=1}^{2\beta} s_t^{(g)} \cdot x_t^{(g)} + \sum_{n=1, n\neq g}^{N} \sum_{t=1}^{2\beta} s_t^{(n)} \cdot x_t^{(g)} + \sum_{t=1}^{2\beta} \xi \cdot x_t^{(g)}. \quad (1)$$

Using Equation 1 and the fact that the chaotic sequences generated by different initial conditions are mutually independent to each other, the mean value of the correlator's output $z_1^{(g)}$, given that the g^{th} user's transmitted bit is +1, can be shown to be (See Appendix A1)

$$E[z_1^{(g)} | (\gamma_1^{(g)} = +1)] = 2\beta \cdot E[(x_t^{(g)})^2],$$

and the variance of is derived to be (See Appendix A2)

$$\begin{aligned} \mathrm{var}[z_1^{(g)} | (\gamma_1^{(g)} = +1)] &= 2\beta \mathrm{var}\lfloor (x_t^{(g)})^2) \rfloor + \beta N_0 E \lfloor (x_t^{(g)})^2 \rfloor \\ &+ \Sigma_{n=1, n\neq g}^{N} 2\beta E[(x_t^{(n)})^2] E[(x_t^{(g)})^2]. \end{aligned}$$

The output of a single correlator is a sum that consists of a large number of independent identical distributed random variables, which is a result of correlation between the 2β samples of the incoming noise corrupted sequence, and the chaotic sequence of a particular user. According to Central Limit Theorem, this sum, containing a large number of independent variables, has a distribution that tends to Gaussian when the number of variables tends to infinity. And an error occurs when $z_1^{(g)} > 0$, given that that transmitted bit, $\gamma_1^{(g)}$, was -1, or vice versa. Therefore, the bit error rate (BER) for the g^{th} user, denoted by

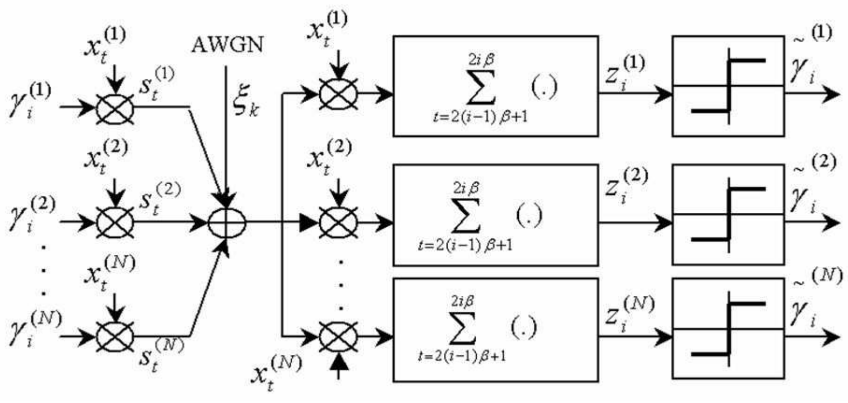

Figure 2: Block diagram of a chaotic communication system

$p^{(g)}$, can be expressed as [11]

$$\begin{aligned} p^{(g)} &= \frac{1}{2}p(z^{(g)} \leq 0|\gamma^{(g)} = +1) + \frac{1}{2}p(z^{(g)} > 0|\gamma^{(g)} = -1) \\ &= \frac{1}{2}\text{erfc}\frac{E[z^{(g)}|\gamma^{(g)} = +1]}{\sqrt{2 \cdot \text{var}[z^{(g)}|\gamma^{(g)} = +1]}}, \end{aligned}$$

where the *error complimentary function*, erfc(.), is defined as in [11]. Assuming that all N users have equal average transmit power P_s, i.e.,

$$P_s = E[(x_t^{(1)})^2] = E[(x_t^{(2)})^2] \ldots = E[(x_t^{(N)})^2],$$

the probability of error for the g^{th} user is (See Appendix A3 for derivations)

$$P^{(g)} = \frac{1}{2}\text{erfc}(\frac{\text{var}[(x_t^{(g)})^2]}{\beta \cdot E^2[(x_t^{(g)})^2]} + \frac{(N-1)}{\beta} + \frac{N_0}{2\beta P_s})^{-\frac{1}{2}}. \quad (2)$$

Let $\Psi = [(x_t^{(g)})^2]/E^2[(x_t^{(g)})^2]$, then, substituting $E_b = 2\beta P_s$ into Equation 2 we may have the general formula for the probability of error

$$BER_{CPSK} = \frac{1}{2}erfc([\frac{\Psi}{\beta} + \frac{(N-1)}{\beta} + (\frac{E_b}{N_o})^{-1}]^{-\frac{1}{2}}), \quad (3)$$

which is slightly different from the expression obtained for the CSK system, and is expressed as [11]

$$BER_{CSK} = \frac{1}{2}erfc([\frac{\Psi}{\beta} + \frac{(2N-1)}{\beta} + (\frac{E_b}{N_o})^{-1}]^{-\frac{1}{2}}). \quad (4)$$

This difference will have significant influence on BER characteristics of these two systems and will give advantage to the CPSK system as we will see in the next sections.

2.3 Analytical and Simulation Results

The CPSK scheme, shown in Figure 2, is simulated using the cubic map and the spreading factor $2\beta = 100$. For accuracy purposes, a minimum of 35 errors were to be detected for each user at each E_b/N_o level. Some of the measurements (i.e. for BER $\leq 10^{-4}$) were done with a higher number of errors, but the simulation time was increased for the orders of magnitude, and the improvement in the accuracy of measurements was not pronounced. The choice of a minimum of 35 errors was determined by following the method described in [1], which states to achieve a BER of 10^{-4}, with a 99% confidence, approximately 30 errors are required to be detected.

The simulator consists of a transmitter, a receiver, and a noise generator, which generates the white noise, based on the noise power, bandwidth of the sequence, and the spreading factor. 20 bits are sent at a time and, the error checking process and the computation of bit error rate take place afterwards. Figure 3 shows the BER results obtained from the analytical Solution 3 and simulations and for different number of users. Figure 4 shows how the BER changes with the number of users, at 5 different E_b/N_o levels.

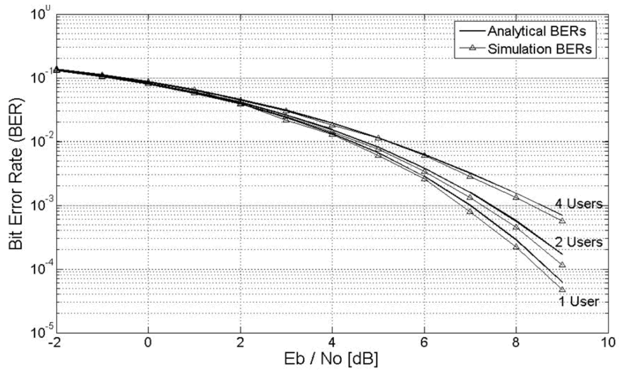

Figure 3: Plot of BER versus E_b/N_o of 1,2 and 4 users CPSK system

Simulation results and analytical solutions are very similar to each other and the BER increases as the E_b/N_o decreases or the number of users increases. Figure 4 shows that as the number of users increases, the change in BER becomes negligible. The increase in BER in the case when the number of users increases and when E_b/N_o is fixed are caused by the inter-user interference in the system. As a conclusion, the analytical Formula 3, can provide good estimations of the performances of the actual system.

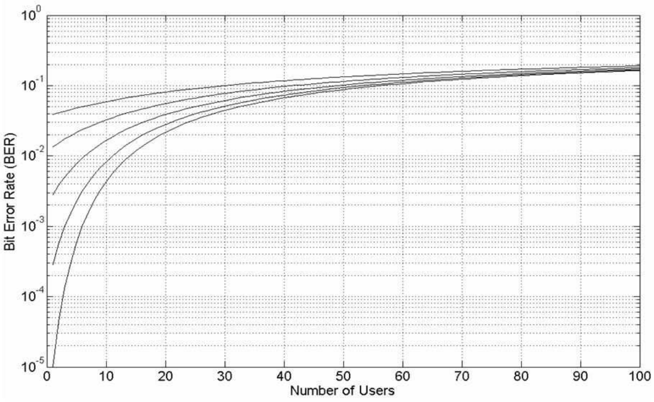

Figure 4: Plot of BER versus number of users in the CPSK system (top to bottom: Eb/No = 2, 4, 6, 8 and 10 dB)

Let's compare the error probability characteristics of CPSK derived in this paper with those of CSK, presented in [11] and, Binary Phase Shift Keying (BPSK), presented in [13] (See Figures 5, 6). In the case of a single user system the BER characteristics of the CPSK system are significantly better than the characteristics of the CSK system, being more than 3 dB for BER = 10^{-3}, as can be seen from Figure 5. Also, the characteristics of the BPSK practically match the characteristics of CPSK, the difference being negligible at BER = 10^{-3}. Therefore, it is possible to design a secure single user system using CPSK modulator that has the BER characteristics comparable with BPSK system.

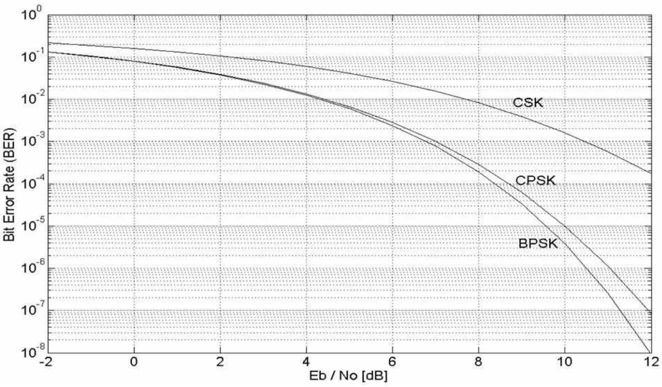

Figure 5: BER comparisons between BPSK, CSK and CPSK (Single user system for each one)

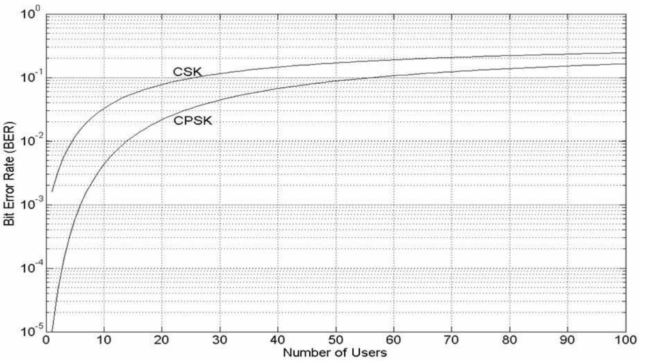

Figure 6: Plot of BER versus number of users, for CSK and CPSK. E_b/N_o is 10 dB

Let us consider the difference between the CPSK and CSK schemes, in terms of the number of users, N. To carry out this comparison (See Figure 7), Equations 3 and 4 are re-arranged to give us the following formulae

$$N_{CPSK} = \frac{\beta}{(erfc^{-1}(2 \cdot \mathrm{BER}))^2} - \Psi + 1 - \beta \cdot (\frac{E_b}{No})^{-1}, \quad (5)$$

$$\begin{aligned} N_{CSK} &= \frac{\beta}{2 \cdot (erfc^{-1}(2 \cdot \mathrm{BER}))^2} \\ &- (\Psi - 1 + 2\beta \cdot (\frac{E_b}{No})^{-1})/2. \quad (6) \end{aligned}$$

Subtracting Equation 6 from Equation 5 gives us

$$N_{diff} = \frac{1}{2}(\frac{\beta}{(\mathrm{erfc}^{-}1(2 \cdot \mathrm{BER}))^2} - \Psi + 1). \quad (7)$$

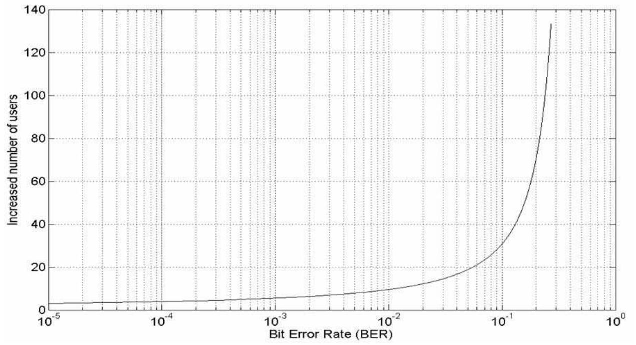

Figure 7: Increased in number of users when comparing the CPSK system with the CSK system, (N_{CPSK4} - N_{CSK}), at various BER

Another point to be noted is that, the increase in number of users is consistent across all levels of noise or bit energy, since Equation 7 does not contain the term E_b/N_o. The number of users that can be supported is significantly higher for the CPSK system, being at least 10 users more than for the CSK system, for a BER of 10^{-2}. This can be considered as an important advantage of the CPSK system that is proposed in this paper.

3 Conclusions

In this paper the background theory and results of simulation of a multi-user chaos-based communication system, called Chaotic Phase Shift Keying, in the presence of white Gaussian noise is presented. The bit error rate formula was derived and theoretical BER curves were compared with the corresponding curves obtained by simulation. It was found that the BER characteristics for the proposed CPSK system are substantially better than that of classical CSK. For a BER of 10^{-3}, the improvement, compared to CSK, in E_b/N_o ratio is about 3.5 dB. The CPSK scheme was found to have a greater system capacity than the classical CSK scheme because it can accommodate more users with the same quality. Also, it was confirmed that the BER curves obtained from software simulations match extremely well the theoretical curves of CPSK.

Possible future work in this field could include the implementation of this proposed system on a hardware platform, such as DSP (digital signal processor) or FPGA (Field Programmable Gate Array) as issues such as processors speeds and finite precision of chaotic samples might degrade the performance of the system.

References

[1] S. M. Berber, "An automated method for ber characteristics measurement," *IEEE Instrumentation and Measurement Technology Conference*, Budapest, Hungary, pp. 1491-1495, May 21-23, 2001.

[2] T. L. Carroll, and L. M. Pecora, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821-825, Feb. 1990.

[3] G. Chen, and T. Ueta, *Chaos In Circuits and Systems*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2002.

[4] L. O. Chua, L. Kocarev, K. S. Halle, U. Parlitz, and A. Shang, "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, pp. 973-977, 1992.

[5] H. Dedieu, M. Hasler, and M. P. Kennedy, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit," *IEEE Transactions on Circuits and Systems Part II*, vol. 40, no. 10, pp. 634-642, 1993.

[6] M. Hasler, and T. Schimming, "Optimal and suboptimal chaos receivers," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 733-746, May 2002.

[7] T. Innami, S. Kodoma, and T. Ushio, "Digital communication systems based on in-phase and anti-phase chaotic synchronization," *Proceedings of 1995 International Symposium of Nonlinear Theory and its Applications*, pp. 133-136, 1995.

[8] Z. Jako, M. P. Kennedy, G. Kis, and G. Kolumban, "FM-DCSK: A robust modulation scheme for chaotic communications," *IEICE Transactions on Fundamentals*, vol. E81-A, no. 9, pp. 1798-1802, Sep. 1998.

[9] M. P. Kennedy, R. Rovatti, and G. Setti, *Chaotic Electronics in Telecommunications*, CRC Press, Boca Raton, 2000.

[10] C. L. Koh and T. Ushio, "Digital communication method based on M-synchronized chaotic systems,"*IEEE Transactions on Circuits and Systems - I*, vol. 44, no. 5, pp. 383-390, May 1997.

[11] F. C. M. Lau, and C. K. Tse, *Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation*, Springer-Verlag, Berlin, 2003.

[12] F. C. M. Lau, A. J. Lawrence, W. M. Tam, and C. K. Tse, "Exact analytical bit error rates for multiple access chaos-based communication system," *IEEE Transactions on Circuits and Systems-II: Analog and digital Signal Processing*, vol. 51, no. 9, pp. 473-481, Sep. 2004.

[13] S. J. Lee, and L. E. Miller, *CDMA System Engineering Handbook*, 1st edition, Artech House Publishers, Boston and London, 1998.

Appendix A: Derivations for $E[z^{(g)}]$

$$\begin{aligned} z_1^{(g)} &= \sum_{n=1}^{N}\sum_{t=1}^{2\beta} s_t^{(n)} x_t^{(g)} + \sum_{t=1}^{2\beta} \xi_t x_t^{(g)} \\ &= \sum_{t=1}^{2\beta}(x_t^{(g)})^2 + \sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta} s_t^{(n)} x_t^{(g)} + \sum_{t=1}^{2\beta} \xi_t x_t^{(g)} \end{aligned}$$

$$\begin{aligned} E[z_1^{(g)}] &= E[\sum_{t=1}^{2\beta}(x_k^{(g)})^2] + E[\sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta}(s_t^{(j)} x_t^{(g)}] + E[\sum_{k=1}^{2\beta} \xi_t x_t^{(g)}] \\ &= \sum_{t=1}^{2\beta} E[(x_k^{(g)})^2] + \sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta} E[(s_t^{(j)} x_t^{(g)}] + \sum_{k=1}^{2\beta} E[\xi_t x_t^{(g)}] \\ &= 2\beta E[(x_t^{(g)})^2] + 0 + 0. \end{aligned}$$

Appendix B: Derivations for var$[z^{(g)}]$

$$\begin{aligned} z_1^{(g)} &= \sum_{n=1}^{N}\sum_{t=1}^{2\beta} s_t^{(n)} x_t^{(g)} + \sum_{t=1}^{2\beta} \xi_t x_t^{(g)} \\ &= \sum_{t=1}^{2\beta}(x_t^{(g)})^2 + \sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta} s_t^{(n)} x_t^{(g)} + \sum_{t=1}^{2\beta} \xi_t x_t^{(g)} \\ &= z_{1_A}^{(g)} + z_{1_B}^{(g)} + z_{1_C}^{(g)}. \end{aligned}$$

$$\begin{aligned} \mathrm{var}[z_1^{(g)}] &= \mathrm{var}[z_{1_A}^{(g)}] + \mathrm{var}[z_{1_B}^{(g)}] + \mathrm{var}[z_{1_C}^{(g)}] \\ &+ \mathrm{cov}(z_{1_A}^{(g)}, z_{1_B}^{(g)}) + \mathrm{cov}(z_{1_A}^{(g)}, z_{1_C}^{(g)}) + \mathrm{cov}(z_{1_B}^{(g)}, z_{1_C}^{(g)}), \end{aligned}$$

where $\mathrm{cov}(z^{(g)}_{1_A}, z^{(g)}_{1_B}) = \mathrm{cov}(z^{(g)}_{1_A}, z^{(g)}_{1_C}) = \mathrm{cov}(z^{(g)}_{1_B}, z^{(g)}_{1_C}) = 0$.

1) $\mathrm{var}[z^{(g)}_{1_A}] = \mathrm{var}[\sum_{t=1}^{2\beta}(x^{(g)}_t)^2] = \sum_{t=1}^{2\beta}\mathrm{var}[(x^{(g)}_t)^2] = 2\beta\mathrm{var}[(x^{(g)}_t)^2]$.

2) $\mathrm{var}[z^{(g)}_{1_B}] = \mathrm{var}[\sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta} s^{(n)}_t x^{(g)}_t] = \sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta}\mathrm{var}[s^{(n)}_t x^{(g)}_t]$, where

$$\begin{aligned}
\mathrm{var}[s^{(n)}_t x^{(g)}_t] &= \mathrm{var}[x^{(n)}_t x^{(g)}_t] \\
&= E[(x^{(n)}_t x^{(g)}_t)^2] - E^2[x^{(n)}_t x^{(g)}_t] \\
&= E[(x^{(n)}_t)^2 (x^{(g)}_t)^2] - E^2[x^{(n)}_t]E^2[x^{(g)}_t] \\
&= E[(x^{(n)}_t)^2]E[(x^{(g)}_t)^2] - E^2[x^{(n)}_t]E^2[x^{(g)}_t] \\
&= E[(x^{(n)}_t)^2]E[(x^{(g)}_t)^2] + 0.
\end{aligned}$$

$$\begin{aligned}
\mathrm{var}[z^{(g)}_{1_B}] &= \sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta}\mathrm{var}[s^{(n)}_t x^{(g)}_t] \\
&= \sum_{n=1,n\neq g}^{N}\sum_{t=1}^{2\beta}E[(x^{(n)}_t)^2]E[(x^{(g)}_t)^2] \\
&= \sum_{n=1,n\neq g}^{N} 2\beta E[(x^{(n)}_t)^2]E[(x^{(g)}_t)^2].
\end{aligned}$$

3)

$$\begin{aligned}
\mathrm{var}[z^{(g)}_{1_C}] &= \mathrm{var}[\sum_{t=1}^{2\beta}\xi_t x^{(g)}_t] = \sum_{t=1}^{2\beta}\mathrm{var}[\xi_t x^{(g)}_t] \\
&= 2\beta\mathrm{var}[\xi_t x^{(g)}_t] = 2\beta\mathrm{var}[\xi_t]\mathrm{var}[x^{(g)}_t].
\end{aligned}$$

Since $\mathrm{var}[(x^{(g)}_t)] = E[(x^{(g)}_t)^2]$ and $\mathrm{var}[\xi_k] = N_0/2$, where N_0 is the noise density, then $\mathrm{var}[z^{(g)}_{1_C}]$ can be given as:

$$\mathrm{var}[z^{(g)}_{1_C}] = 2\beta N_0/2 \cdot P^{(g)}_c = \beta N_0 E[(x^{(g)}_t)^2].$$

Therefore, the $\mathrm{var}[z^{(g)}_i]$ is

$$\begin{aligned}
\mathrm{var}[z^{(g)}_1] &= \mathrm{var}[z^{(g)}_{1_A}] + \mathrm{var}[z^{(g)}_{1_B}] + \mathrm{var}[z^{(g)}_{1_C}] \\
&+ \mathrm{cov}(z^{(g)}_{1_A}, z^{(g)}_{1_B}) + \mathrm{cov}(z^{(g)}_{1_A}, z^{(g)}_{1_C}) + \mathrm{cov}(z^{(g)}_{1_B}, z^{(g)}_{1_C}) \\
&= 2\beta\mathrm{var}[(x^{(g)}_k)^2] + \sum_{n=1,n\neq g}^{N} 2\beta E[(x^{(n)}_t)^2]E[(x^{(g)}_t)^2] \\
&+ \beta N_0 E[(x^{(g)}_t)^2].
\end{aligned}$$

Appendix C: Derivations for $P^{(g)}$

$$\begin{aligned}
P^{(g)} &= \frac{1}{2}\mathrm{erfc}\frac{E[z^{(g)}|\gamma^{(g)} = +1]}{\sqrt{2\cdot\mathrm{var}[z^{(g)}|\gamma^{(g)} = +1]}} \\
&= \frac{1}{2}\mathrm{erfc}(\frac{2\beta P_5}{V}) \\
&= \frac{1}{2}\mathrm{erfc}\{(\frac{V_1}{4\beta^2 P_5^2})^{-\frac{1}{2}}\} \\
&= \frac{1}{2}\mathrm{erfc}\{(\frac{\mathrm{var}[(x^{(g)}_t)^2]}{\beta P_5^2} + \frac{(N-1)}{\beta} + \frac{N_0}{2\beta P_5})^{-\frac{1}{2}}\} \\
&= \frac{1}{2}\mathrm{erfc}\{(\frac{\mathrm{var}[(x^{(g)}_t)^2]}{\beta E^2[(x^{(g)}_t)^2]} + \frac{(N-1)}{\beta} + \frac{N_0}{2\beta P_5})^{-\frac{1}{2}}\} \\
V &= \sqrt{2(2\beta\mathrm{var}[(x^{(g)}_t)^2]) + \sum_{n=1,n\neq g}^{N} 2\beta P_5^2 + \beta N_0 P_5)} \\
V_1 &= 4\beta\mathrm{var}[(x^{(g)}_k)^2] + 4\beta(N-1)(P_5)^2 + 2\beta N_0 P_5.
\end{aligned}$$

Stevan Berber was born in Stanisic, Serbia in 1950. He completed his undergraduate studies in electrical engineering in Zagreb, master studies in Belgrade, and PhD studies in Auckland, New Zealand. Before coming to the academic world he was working nearly 20 years in research institutions and in telecommunication industry having research interests in mobile communication systems and digital transmission systems and ISDN networks. At present Stevan is with the University of Auckland in New Zealand. His research interests are in the field of digital communication systems (modulation and coding theory and applications), in particular CDMA systems and wireless computer and sensor networks. His teaching interests are in communication systems, information and coding theory, digital signal processing and computer networks. He is an author of more than 60 referred journal and international conference papers and 7 books. Stevan has been leading or working on a number of research and industry projects.

Gobindar S. Sandhu is currently a PhD student in the Department of Electrical and Computer Engineering at the University of Auckland, New Zealand. He received a Bachelor of Engineering degree in Electrical and Electronics Engineering with First Class Honours from University of Auckland. His research interests include CDMA systems and secure communications.