CHAOTIC –PULSE-POSITION MODULATION: AN IMPROVED THIRD PARTY INTRUSION SCHEME USING EKF

Franck O. Hounkpevi and Edwin E. Yaz

Department of EECE, Marquette University, Milwaukee WI 53201, USA
Email: franck.hounkpevi@mu.edu, edwin.yaz@mu.edu

Abstract: In a recent paper we have introduced a third party intrusion scheme to decode the transmitted message in chaotic-pulse-position modulation using a Kalman Filter. In the present work, we improve the design of this intrusion scheme to not only allow us to recover the transmitted message but also enable the estimation of the signal power m. This is a much more complicated task than the past one as the system model obtained becomes nonlinear. To achieve this goal, we have used a modified version of the Extended Kalman Filter fed with a polynomial approximation. We have conducted experiments using the quadratic map and the logistic map. The outcome of these experiments shows that both the original message and the signal power m can be effectively recovered. The Bit Error Rate performance of this scheme is compared to that of the chaotic-pulse-position modulation for different Signal to Noise Ratios. Also the efficacy of estimation of the value of m is shown as well as the degree of the polynomial map used. Overall, these results cast a doubt on the security of the chaotic-pulse-position modulation scheme.

Keywords: Communication systems, nonlinear systems, estimation theory, extended Kalman filters, chaos theory.

1. INTRODUCTION

Chaotic signals may have a significant impact on tomorrow's spread spectrum communication systems. From the random-like nature of these signals to their sensitivity to initial conditions, these signals offer a wide range of promising properties which may revolutionize the field of secure communication. Since the possibility of using chaotic signal for digital modulation was mentioned in (Abel, and Schwarz, 2002), various chaotic modulation schemes have been introduced to guarantee security (Rulkov, et al., 2001; Cheong, et al., 2003; Kolumban, et al., 1998a). In this paper we will be interested in Chaotic-Pulse-Position Modulation (CPPM).

Recently, in (Hounkpevi, and Yaz, 2004) we have raised a question regarding the security claim of CPPM. As security is a key reason for using chaotic signals in spread spectrum digital communications, we find it essential to address this particular problem in any proposed chaotic modulation system. At the present time, there are very few results that address this important security issue in chaotic communications. In fact, most articles on chaotic modulation so far, are confined to testing if the message can be regenerated at the receiver and if the Bit Error Rate (BER) is at an acceptable level for some specified values of the Signal to Noise Ratio (SNR). Mostly, unproven security claims rely on the fact that the signal is random-like (Hasler, and Maistrenko, 1997; Kolumban, et al., 1998b). In our

previous work (Hounkpevi, and Yaz, 2004), we have directed our attention to the CPPM modulation scheme. We have performed experiments to test if CPPM is as secure as claimed. In these experiments, we have shown that it is possible to recover the transmitted message as an unintended third party without knowing either the initial condition or the chaotic map used to transmit the message.

In that work (Hounkpevi, and Yaz, 2004), we assumed that the signal power was known or that at least the sign of its coefficient was known. This assumption led to a linear (Kalman) filtering solution to the demodulation problem. In the present paper, in addition to the original message, also the value of the signal power (or equivalently the coefficient of the message signal) is being estimated. Although this is an extension of our previous work, it is a much more complicated task as the new model is nonlinear and Kalman filtering can no longer be used as in (Hounkpevi, and Yaz, 2004). We apply the Extended Kalman Filter to this nonlinear estimation problem with some modifications to enhance its convergence properties. We have performed simulation experiments using CPPM at the transmitter and at the receiver; we have used our Modified EKF fed with a polynomial approximation to recover the original message. The results obtained show that not only can we recover the message but we can also estimate the power of the signal. The Bit Error Rate (BER) for various SNRs is shown and compared to that of CPPM. Parameter estimation errors are also shown to prove the feasibility of this task. Finally, the degree of the polynomial map is estimated.

In section 2 a brief introduction to CPPM is given. In Section 3 we present our third party intrusion scheme. Simulation results are in section 4. Section 5 contains conclusions.

2. CPPM

In this modulation scheme, a chaotic signal in the form of a pulse train is sent across the channel. First, a pulse train with inter-pulse intervals determined by a chaotic map $F(\cdot)$ dynamics is generated by a chaotic pulse generator according to:

$$T_n = F\left(T_{n-1}\right) \tag{1}$$

The generated pulse train is then used as a carrier which modulates a binary message signal $S_n\left(\pm 1\right)$:

$$T_n = F\left(T_{n-1}\right) + d + mS_n \tag{2}$$

where m is the signal amplitude, and d a constant delay.

At the decoder, the consecutive time interval T_{n-1} and T_n are measured and the estimate of the message is generated by

$$\hat{S}_n = \left(T_n - F\left(T_{n-1}\right) - d\right)/m \tag{3}$$

The nonlinear function and the parameters should be the same in the receiver and the transmitter for the encoded message to be recovered. Therefore, it can be argued that an unauthorized receiver who does not know the dynamics of the system or the initial condition cannot recover the transmitted message. It is this claim that is the subject of our investigation here.

3. THIRD PARTY INTRUSION SCHEME FOR CPPM

In reality, the received signal is equal to the modulated message plus a channel noise W_n assumed to be AWGN (Additive White Gaussian Noise) with zero mean and covariance W . A realistic model of the third party intruder assumes no knowledge of the chaotic map used in the transmitter, the initial condition of the chaotic signal T_0 , the delay d , or the amplitude m of the message (or m^2 the signal power, assuming that +1, -1 are equally likely to be transmitted). In this development, the message S_n will be modeled as a binary distributed random variable. By approximating the map by a second degree polynomial $a + bx + cx^2$, the signal at the receiver is

$$y_n = a_n + b_n y_{n-1} + c_n y_{n-1}^2 + mS_n + W_n \tag{4}$$

To be able to estimate m together with the parameters a , b , c of the map, we set up the signal model as follows.

$$\begin{cases} \begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \\ m_{n+1} \end{bmatrix} = \begin{bmatrix} a_n \\ b_n \\ c_n \\ m_n \end{bmatrix} \\ y_n = \left[1, y_{n-1}, y_{n-1}^2, S_n\right] \begin{bmatrix} a_n \\ b_n \\ c_n \\ m_n \end{bmatrix} + W_n \end{cases} \tag{5}$$

The state to be estimate is now $\begin{bmatrix} a_n \\ b_n \\ c_n \\ m_n \end{bmatrix}$, and the resulting estimation problem is more complicated to solve as the observation equation contains state multiplicative noise. This poses a nonlinear estimation problem with no known globally optimal solution.

Let:

$$C_n = [1, y_{n-1}, y_{n-1}^2, S_n] , \tag{6}$$

$$X_n = \begin{bmatrix} a_n \\ b_n \\ c_n \\ m_n \end{bmatrix} \tag{7}$$

we can rewrite our system as

$$\begin{cases} X_{n+1} = X_n \\ Y_n = C_n X_n + W_n \end{cases} \tag{8}$$

where C_n is time-varying and stochastic.
To estimate the state, we separate C_n into two parts:

$$C_n = \bar{C}_n + \tilde{C}_n \tag{9}$$

where $\bar{C}_n = [1, y_{n-1}, y_{n-1}^2, 0]$ is the mean value or the deterministic component and $\tilde{C}_n = [0,0,0,S_n]$ is the stochastic component.
EKF state estimate update equation is given by the recursion

$$\hat{X}_{n+1} = \hat{X}_n + K_n\left(Y_n - \bar{C}_n \hat{X}_n\right) \tag{10}$$

K_n is the Kalman gain obtained by

$$K_n = P_n \bar{C}_n^T \left(\bar{C}_n P_n \bar{C}_n^T + E\{S_n^2\} P_n(4,4) + W\right)^{-1} \tag{11}$$

and P_n is the estimation error covariance obtained from

$$P_{n+1} = A_n P_n A_n^T + V - A_n P_n \bar{C}_n^T \left(\bar{C}_n P_n \bar{C}_n^T + E\{S_n^2\} P_n(4,4) + W\right)^{-1} \bar{C}_n P_n A_n^T \tag{12}$$

and $P_n(4,4)$ is the 4 - 4 element of P_n.
Upon substitution, these two equations yield:

$$K_n = P_n \bar{C}_n^T \left(\bar{C}_n P_n \bar{C}_n^T + P_n(4,4) + W\right)^{-1} \tag{13}$$

and

$$P_{n+1} = A_n P_n A_n^T + V - A_n P_n \bar{C}_n^T \left(\bar{C}_n P_n \bar{C}_n^T + P_n(4,4) + W\right)^{-1} \bar{C}_n P_n A_n^T \tag{14}$$

Due to unobservability problems, we have modified $\bar{C}_n$ to $\bar{C}_n = [1, y_{n-1}, y_{n-1}^2, \gamma_n]$ where γ_n is a zero mean noise with a very small variance. This also helps to guarantee the error covariance matrix P_n does not stop prematurely. In our simulation, a computer generated value for γ_n is used.

Under this condition, equation (10) gives us the minimum variance estimate of the parameters a, b, c, and m.
After parameter estimation with EKF, the original message is recovered by:

$$\hat{S}_n = \begin{cases} 1, & if \left(T_n - \hat{a} - \hat{b} T_{n-1} - \hat{c} T_{n-1}^2\right)/\hat{m} \geq 0 \\ -1, & if \left(T_n - \hat{a} - \hat{b} T_{n-1} - \hat{c} T_{n-1}^2\right)/\hat{m} < 0 \end{cases} \tag{15}$$

Two well known chaotic maps have been used in these experiments; the quadratic and the logistic map. The BER performance for different SNRs is evaluated and compared to that of the original CPPM. The normalized error between the actual value and the estimated value of m is also given. In the following section, we describe the simulation set up and the results obtained.

4. SIMULATION EXPERIMENTS

The quadratic map used is $x_{n+1} = x_n^2 - g$ where we selected $g = 2$, and the logistic map used is $x_{n+1} = g x_n (1 - x_n)$, where $g = 3.741$. We computed the BER as the ratio of the number of samples that were incorrectly decoded to the total number of samples. The SNR was determined as the ratio of the signal power to the channel noise power. For each of these maps, the BER is computed for different values of the SNR and is compared to the simulated BER performance obtained with CPPM (Rulkov, et al., 2001). The BER vs. SNR for the quadratic map is given in Figure 1. The BER vs. SNR for the logistic map is shown in Figure 2.

For both maps, we can see that the BER of our scheme is competitive with that of CPPM. For high SNRs, which correspond to low noise power, CPPM performs slightly better than our scheme. This is predictable as the receiver at CPPM has the exact value of the parameter and our scheme does not (we generate estimates). For low SNRs, which correspond to high noise power, our scheme performs slightly better than CPPM. This is due to the fact that noise has corrupted the received signal and the parameters at the CPPM receiver do not match exactly that of the transmitted signal any more. However, due to its noise reduction power, EKF has been able to reduce the noise and therefore resulted in a better estimate.

This shows that we have been able to recover the message as an unintended third party using this new scheme. We have also plotted the error resulting from the estimation of m. Shown in Figure 3 is the normalized error for the quadratic map, and in Figure 4 is the normalized error for the logistic map. It is clear that this error is very small (in the order of 10^{-3}) and consequently, the estimation was successful. We have therefore achieved our goal. Figures 5–10 show the normalized error between the estimate and the true value for the parameters of the chaotic map by EKF.

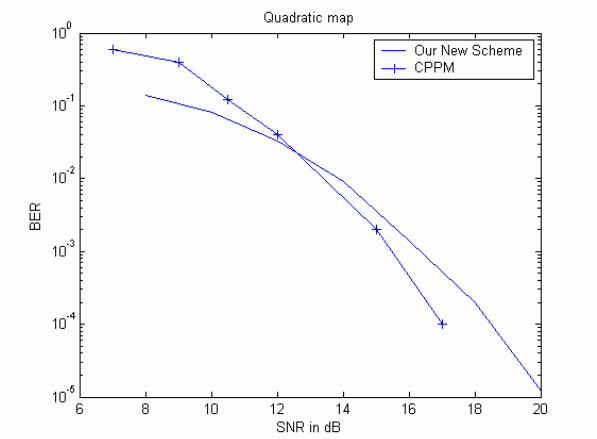

Figure 1. BER of the new intrusion scheme - quadratic map

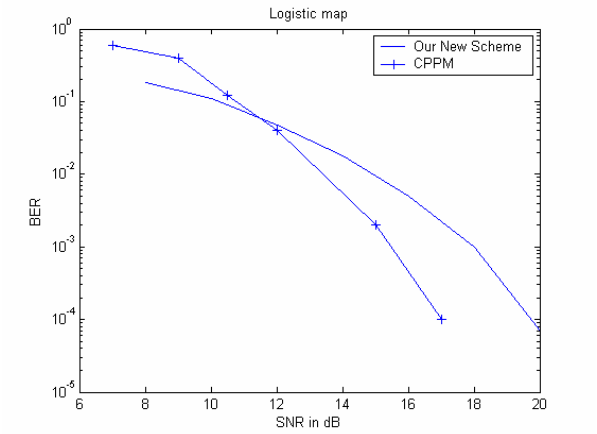

Figure 2. BER of the new intrusion scheme - logistic map

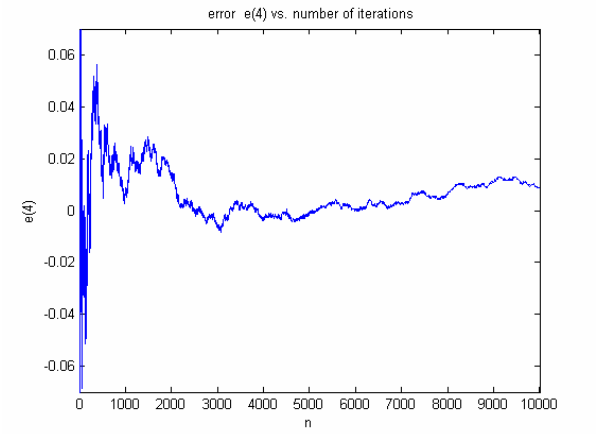

Figure 3. Error for estimation of m - quadratic map

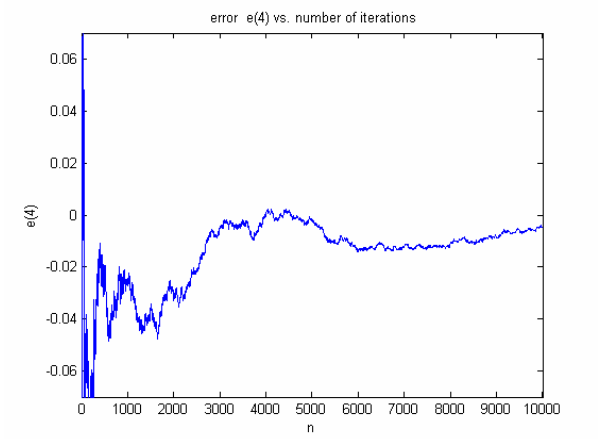

Figure 4. Error for estimation of m - logistic map

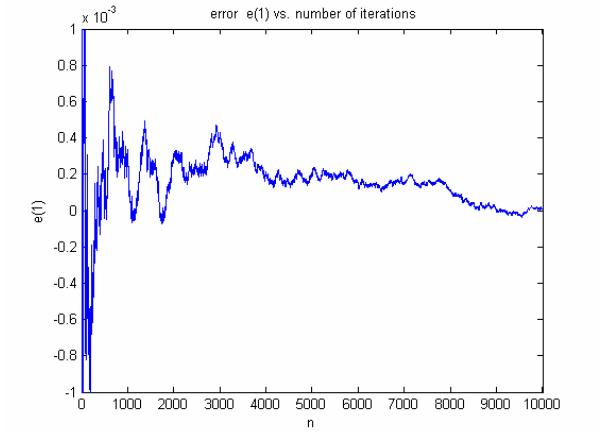

Figure 5. Error for estimation of a- quadratic map

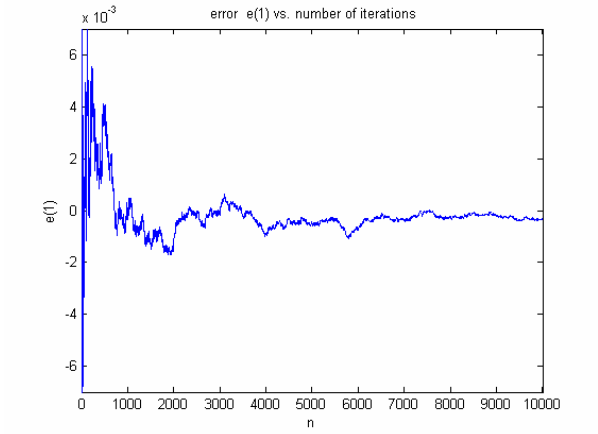

Figure 6. Error for estimation of a – logistic map

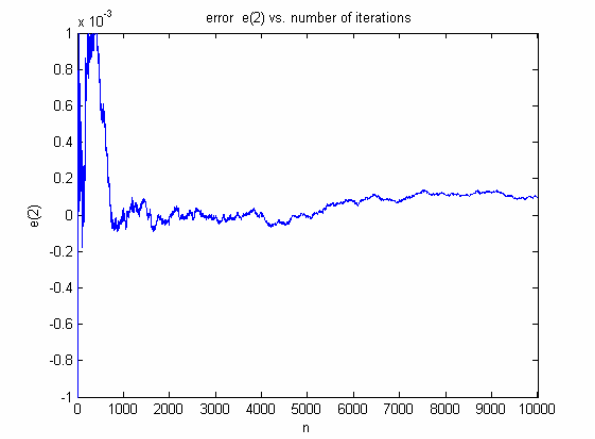

Figure 7. Error for estimation of b - quadratic map

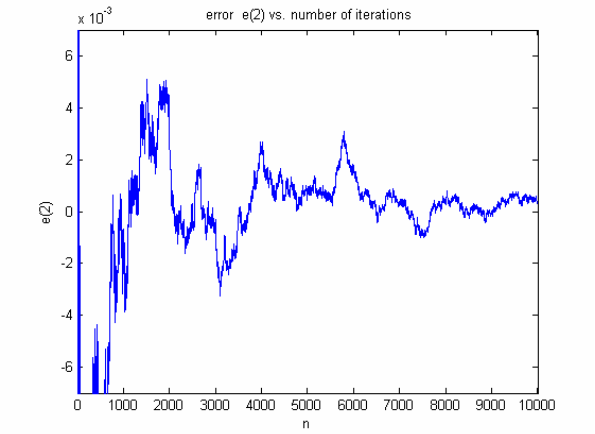

Figure 8. Error for estimation of b - logistic map

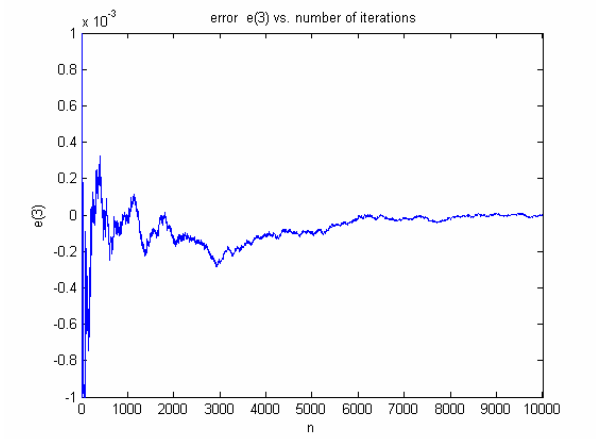

Figure 9. Error for estimation of c - quadratic map

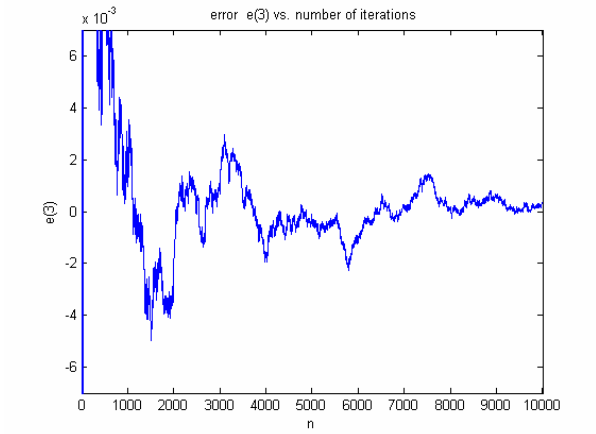

Figure 10. Error for estimation of c - logistic map

Table 1. Error resulting from estimating the degree of the chaotic map

Chaotic map	1st order	2nd order	3rd order	4th order	5th order
Quadratic: 1.7	0.0084	1.02e-004	9.15e-005	1.21e-004	1.33e-004
Quadratic: 1.75	0.0367	8.56e-005	6.81e-005	6.24e-005	7.51e-005
Quadratic: 1.77	0.0091	1.12e-004	1.20e-004	1.31e-004	1.81e-004
Quadratic: 1.8	0.0901	5.87e-005	7.31e-005	8.71e-005	8.01e-005
Quadratic: 1.85	0.0111	2.14e-004	2.70e-004	1.51e-004	1.22e-004
Quadratic: 1.88	0.0308	9.05e-005	8.21e-005	8.14e-005	7.30e-005
Quadratic: 1.9	0.0042	8.94e-005	7.16e-005	7.12e-005	6.61e-005
Quadratic: 1.95	0.0122	3.03e-004	3.21e-004	1.77e-004	1.25e-004
Quadratic: 1.98	0.0015	9.79e-005	8.18e-005	8.07e-005	8.33e-005
Quadratic: 1.99	0.0096	1.02e-004	8.32e-005	9.22e-005	7.85e-005
Logistic: 3.741	0.0031	9.13e-005	1.53e-004	4.45e-004	4.32e-004
Logistic: 3.8	0.0056	1.71e-004	1.84e-004	1.10e-004	1.42e-004
Logistic: 3.85	0.0012	6.07e-005	4.45e-005	4.32e-005	3.31e-005
Logistic: 3.9	0.0017	8.13e-005	8.02e-005	8.78e-005	8.61e-005
Logistic: 3.93	0.0024	9.36e-005	8.15e-005	7.19e-005	1.91e-004
Cubic: -2.3	0.0715	1.12e-004	9.61e-005	9.24e-005	6.71e-005

The third party intrusion scheme assumes no knowledge of the chaotic map used which implies no knowledge of the degree of the map. So how did we know that we can use an EKF fed with a second order approximation in the above simulation? The answer to this question is that the first task to be performed by our intrusion scheme is the estimation of the degree of the chaotic map. This is done by using a bank of EKFs placed at the receiver, each having polynomial of different degrees. We provided a set of simulation experiments to show that these simulations can be done. In this simulation, we consider a bank of 5 EKFs each having polynomial with degree varying from 1 to 5. The test set that we use consists of 16 different maps: 10 quadratic maps $x_{n+1} = x_n^2 - g$ (where g =1.7, 1.75, 1.77, 1.8, 1.85, 1.88, 1.9, 1.95, 1.98, 1.99), 5 logistic maps $x_{n+1} = gx_n(1-x_n)$, (where g = 3.741, 3.8, 3.85, 3.9, 3.93) and 1 cubic map $x_{n+1} = gx_n(1-x_n^2)$, (where g =-2.3). In each case, the EKF having the polynomial whose degree corresponds to that of the map leads to the minimum error ($\varepsilon = \frac{1}{N}\sum_{i=1}^{N}\left|y_i - \hat{y}_i\right|$, $N = 10000$) with the smallest order. This is illustrated in Table 1. With the degree of the map successfully estimated, we have completed the set of tasks that need to be performed for the effective recovery of the transmitted message by an unintended receiver.

5. CONCLUSION

In a previous paper, some security issues related to the use of chaotic-pulse-position modulation were considered. It was shown that it is possible to recover the message as an unintended third party without knowing the initial state or the chaotic map used to transmit the message. In this paper, which is an extension of our previous work, we have shown that it is possible to recover the original message based on less knowledge of the underlying modulation dynamics. Experimental results obtained for two major chaotic maps; the quadratic and the logistic maps truly question the security feature of CPPM. In conclusion we need to point out that the goal of our research is not to describe CPPM as a poor modulation scheme. However, we hope that our contribution will point out to a security risk and therefore will result in more research to increase the security of this communication scheme.

REFERENCES

Abel A., W. Schwarz (2002). Chaos Communications-Principles, schemes, and system analysis, *Proceedings of IEEE*, vol.90, no.5.

Cheong K. Y., F.C. M. Lau and C.K. Tse (2003). An M-ary transmission scheme for chaotic communication, *Proceedings, Regional Inter-University Postgraduate Electrical and Electronic Engineering conference (RIUPEEEC)*, Hong Kong, China, pp. 149-105.

Hasler M. and Y. Maistrenko(1997). An introduction to synchronization of chaotic systems: Coupled skew tent maps, *IEEE Trans on Circuits and Sys*., Vol. 44 pp. 856-866.

Hounkpevi F. O., E. E. Yaz (2004). Chaotic-pulse-position modulation: A third party intrusion scheme, *Proceedings. Of IEEE Electro/Information Technology Conference*, Milwaukee, WI (to appear).

Kolumban G., G. Kis, Z. Jako and M.P. Kennedy (1998a). FM-DCSK: A robust modulation scheme for chaotic communication, *IEICE Trans. Fund*., vol. E81–A, pp. 1798-8002.

Kolumban G., M. P. Kennedy and L. Chua (1998b). The role of synchronization in digital communication using chaos, *IEEE Trans. on Circuits and Sys*., vol.45, pp. 1129-1140.

Rulkov N. F., M. M. Sushchik, L. S. Tsimring, and A. R. Volkovskii (2001). Digital communication using chaotic pulse position modulation, *IEEE Trans. on Circuits and Sys*, vol. 48, pp. 1436-1444.