Low-Power Realizations of Secure Chaotic Communication Schemes

Cristinel Ababei, Radu Marculescu

Department of Electrical and Computer Engineering
University of Minnesota
Minneapolis, MN 55455
E-mail: ababei@ece.umn.edu

Abstract -- *The objective of this paper is to present a low-power realization of a Chaotic Communication (CC) system. We propose a CC scheme that represents an efficient solution in terms of complexity, power consumption, information transmission security, and performance. The newly proposed system is realized by cascading two circuits, namely a nonlinear third order IIR filter and a modified Colpitts oscillator. It is shown that the latter circuit behaves chaotically and the synchronization mechanism can be used to build a complete communication system. The experimental results show that, in terms of power dissipation, the scheme that we propose performs much better (about 2.5 times) compared to other implementations proposed so far for CC. Directions to further decrease the power consumption are suggested.*

Keywords: chaotic communication, low-power chaotic circuits, Colpitts oscillator, nonlinear filters, synchronization, security.

I. Introduction

Chaotic communication (CC) techniques have received much attention in the last few years [1], [6], [9]. Chaotic signals offer an alternative to the classical spread spectrum techniques. Generally speaking, *CC* systems are based on the same idea as the Code Division Multiple Access (CDMA) systems [14]. The role of the random signal in CDMA techniques is played by a chaotic signal which can produce a similar spectrum. The security of *CC* schemes comes from the fact that the information is "hidden" in the chaotic carrier by different techniques like summation, modulation, or shifting [5]. This way, the signal transmitted over the channel becomes a wideband signal which carries the signature of the information signal and is uniquely determined by the parameters of the chaotic generator. Recovering the information is achieved by employing the *synchronization* of two chaotic circuits (transmitter and receiver) without transmitting any information about the initial state of the chaotic circuit used at the transmitter [13].

So far, most of the research has been focused on studying chaotic systems with respect to: *hiding* the information signal in the chaotic carrier, *recovering* the information at the receiver, *security* of the information transmission, *robustness* with respect to the parameter variation or the noisy real communication channels, *sensitivity* to initial conditions of the chaotic generators [5].

To the best of our knowledge, however, there is no study regarding the power consumption of the basic blocks involved in a *CC* system and the alternatives which can be considered to reduce the overall power dissipation. This work tries to link the choice of the *CC* scheme to the issue of low-power consumption by offering a practical solution which represents an efficient solution in terms of complexity, power consumption, information transmission security, and performance. Bringing the power dissipation issue into the picture is a completely new perspective on *CC* systems with potentially deep implications for mobile multimedia applications. In many cases, if the transmission rate is very high, hardware encryption solutions are preferred to classical software encryption techniques. The *CC* system that we propose fits very well these scenarios, offering a low-power, secure, and high-performance solution. Our chaotic circuit can be easily implemented into a dedicated integrated circuit which can be later implanted as an *encryption* module in many indoor/outdoor wireless communication systems.

A. Contribution of this paper

In this paper, we address the novel issue of power dissipation in *CC* systems. As main contribution, we propose a power-efficient solution based on using third order *IIR* filters and a modified version of the standard Colpitts oscillator. Our analysis focuses essentially on the Colpitts oscillator which may represent the basic cell in any *CC* scheme. The ultimate goal is to come to a better understanding of the intimate relationship between the choice of a *CC* system and its power dissipation, information transmission security, and performance. As experiments show, this new scheme represents an efficient solution in terms of complexity, power consumption, information transmission security, and performance.

B. Paper organization

Section II presents our proposed communication scheme. Sections III provides a detailed analysis of the chaotic circuit which is the core of our communication scheme (i.e. the modified Colpitts oscillator). Practical considerations, power consumption analysis, and experimental results are presented in Section IV. Security issues and directions to decrease the power consumption are also discussed. We conclude by summarizing our main contribution.

II. The Chaotic Communication System

In this section, we discuss our proposed communication scheme and outline its specific novel features. Our proposed *CC* system is a synchronization-based scheme; its block diagram is shown in Fig.1.

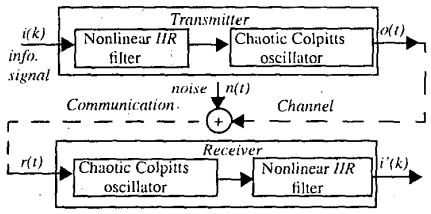

Fig.1 The block diagram of the communication system

The transmitter comprises two cascaded dynamical systems: a nonlinear digital filter[1] cascaded with a modified Colpitts oscillator. The idea of cascading these two systems is to obtain a higher level of security of the information transmission. The information signal *i(k)* is hidden in the chaotic signal *o(t)* generated by the modified Colpitts oscillator at the transmitter. The output of the nonlinear *IIR* filter [10], through which the information signal is first processed, controls the chaotic switching in the Colpitts oscillator. The choice of a Colpitts oscillator is motivated by its simplicity and reduced power consumption. Moreover, its wide bandwidth [11] and rich dynamical (chaotic) behavior, make it broadly used in communications. Per overall, the proposed scheme is an efficient

1. Under certain conditions, nonlinear digital filters exhibit complex behavior. This complex behavior is commonly referred to as being chaotic [2].

0-7803-6253-5/00/$10.00 ©2000 IEEE.

solution for low-power applications where a certain level of security is required.

Since our focus is on the modified Colpitts oscillator and its power dissipation, in the next section, we study the oscillator in more detail. We do not study the filter structure herein, due to space limitations. However, in Section IV, we will discuss some security issues and present simulation results for the whole *CC* scheme.

III. The Modified Colpitts Oscillator-based Chaotic Communication Scheme

A. The block diagram

The block diagram of the communication scheme based on the modified Colpitts oscillator is presented in Fig.2. It is a chaotic switching communication scheme [12], in which the transmitter consists of a chaotic generator which has one of its parameters switched according to the binary information signal *i(k)*. The receiver contains two copies of the transmitter generator each corresponding to one of the two switched parameters. The information signal can be recovered from the error signals $e_1(t)$ and $e_2(t)$. We note that this general communication scheme can be further simplified by building the receiver only from the generator characterized by parameter *P*. This will still allow us to recover the information signal by saving power consumption at the expense of a slightly decreased reliability of the communication system.

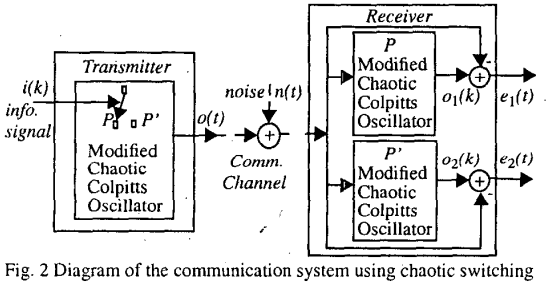

Fig. 2 Diagram of the communication system using chaotic switching

The detailed schematic of the new proposed version of the Colpitts oscillator is shown in Fig.3.*a*. The difference from the standard scheme in [8] is that a resistor (r_1) is added to the emitter of the Bipolar Junction Transistor (BJT) *Q*. This change in the schematic has two main advantages: First, since the oscillator is divided in two subcircuits by means of resistor r_1, the oscillator at the receiver can be split in two separated units; thus the *decomposition* into subsystems technique [5] becomes applicable (Fig.3.*b*). Then, the technique of decomposition into subsystems requires minimal additional circuitry compared to other solutions (e.g. the inverse system technique [5]). This, complemented by the simplicity of the oscillator itself, will determine a minimal power consumption of the transmitter-receiver system.

B. Analysis of the transmitter-receiver system

The three state equations which characterize the dynamics of the modified Colpitts oscillator in Fig. 3.*a* are:

$$\begin{cases} \dot{x} = \frac{1}{C_1} z - \frac{\beta}{C_1} f(v_{BE}) \\ \dot{y} = -\frac{1}{R_E C_2} y + \frac{1}{C_2} z - \frac{V_{EE}}{R_E C_2} + \frac{1}{C_2} f(v_{BE}) \\ \dot{z} = -\frac{1}{L} x - \frac{1}{L} y - \frac{(R_L + r_1)}{L} z + \frac{V_{CC}}{L} - \frac{r_1}{L} f(v_{BE}) \end{cases} \quad (1)$$

In the above equations, the state variables *x*, *y*, and *z* are the voltage drops on the two capacitors C_1 and C_2 and the current through *L*, respectively. The operator "." in the left hand side denotes the derivative operator with respect to time.

The nonlinearity $f(v_{BE})$ models the base-emitter junction of the active device and is given by the equation:

$$f(v_{BE}) = I_S\left(\exp\left(\frac{v_{BE}}{V_T}\right) - 1\right) \quad (2)$$

where, I_S denotes the saturation junction current; it usually has a magnitude of $I_S = 10^{-11} \ldots 10^{-13}$ *A*. $V_T = KT/q$ denotes the thermal voltage, and equals 26 *mV* at room temperature. The base-emitter voltage drop v_{BE} is given by:

$$v_{BE} = -y - r_1(z + f(v_{BE})) \quad (3)$$

The receiver is composed of two subsystems (*A* and *B* in Fig. 3.*b*), characterized by:

subsystem A:

$$\begin{cases} \dot{x}_A = \frac{1}{C_1} z_A - \frac{\beta}{C_1} f(v_{BE_A}) \\ \dot{z}_A = -\frac{1}{L} x_A - \frac{1}{L} y - \frac{(R_L + r_1)}{L} z_A + \frac{V_{CC}}{L} - \frac{r_1}{L} f(v_{BE_A}) \end{cases} \quad (4.a)$$

subsystem B:

$$\dot{y}_B = -\frac{1}{R_E C_2} y_B + \frac{1}{C_2} z_A - \frac{V_{EE}}{R_E C_2} + \frac{1}{C_2} f(v_{BE_B}) \quad (4.b)$$

The subsystem *A* is driven by the signal *y* trasmitted over the communication channel by the transmitter (eq. (1)); in turn, the subsystem *B* is driven by *A*. We note that, in our discussion, the additive noise of the channel *n(t)* is considered negligible; this is why the received signal *y* in (4.a) is identical with the transmitted signal *y* in (1). It can be mathematically proven that, *the receiver synchronizes with the transmitter; that is, the receiver described by the equations (4) synchronizes with the transmitter described by the equations (1) and the synchronization is stable with respect to the initial conditions of the two circuits.*

C. Numerical simulations of the communication scheme

To qualitatively asses the chaotic behavior of the overall system, the transmitter-receiver system (Fig.3.*b*) is simulated at block-diagram level with Matlab. By doing so, we have observed that: 1) the transmitter still behaves chaotically for small values of r_1, 2) asymptotic synchronization is achieved, and 3) reliable information transmission is possible. The parameter chosen to be switched is the resistance R_E. This is because the chaotic signal transmitted over the channel, when R_E is switched between two values, does not significantly change its bias component. Such a change would give the possibility to a cryptanalyst to easily break the security of the system. The two values of R_E are R_E=400 Ω and R_E'=350 Ω (parameters *P* and *P'* in Fig.2, respectively). The information signal *i(k)* (which, for the sake of simplicity, is a simple rectangular pulse) and the signal transmitted over the channel *y(t)* are shown in Fig.4.*a.b*.

When the chaotic oscillator, at the transmitter, is characterized by R_E'=350 Ω (bit "0" is transmitted), the receiver, which is characterized by R_E=400 Ω, does not synchronize with the transmitter. In this situation, the error signal Δ*y* (Fig.4.c) diverges towards a non-zero value. When a bit "1" is transmitted (the transmitter has R_E=400 Ω as the receiver does) the error signal Δ*y* converges to zero. Thus, using a threshold comparator, a

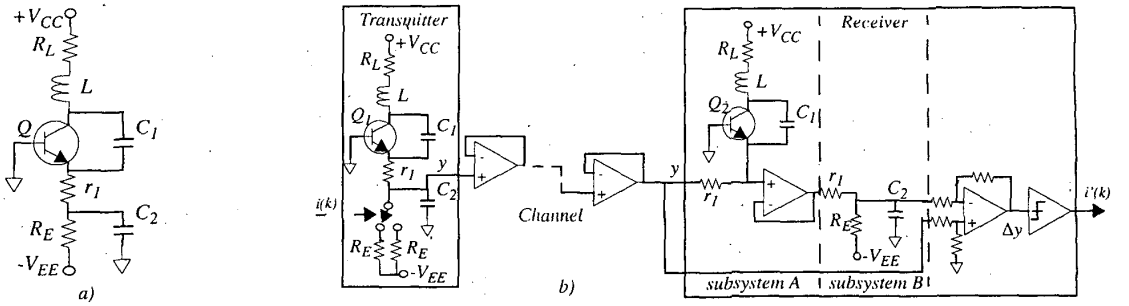

Fig.3 Block diagram of the modified Colpitts oscillator *a)* and block diagram of the transmitter-receiver system *b)*

decision whether or not the chaotic carrier corresponding to parameter P or P' is transmitted can be made. The recovered information signal $i'(k)$ (Fig.4.*d*) is obviously identical to that used for switching at the transmitter, but it has a small phase shift which depends on the threshold chosen for the comparator. The chaotic synchronization process can be seen in Fig.5.a, where the voltage drop on capacitor C_2 (y_B) at the receiver is plotted vs. the voltage on capacitor C_2 at the transmitter (y). Finally, the state space trajectory projection on the x-y plane (at the transmitter) is shown in Fig.5.b. It can be seen that the suspected attractor is in perfect agreement to the one in [8], which implies the chaotic nature of the dynamics of the transmitter.

To conclude, the modified Colpitts oscillator behaves chaotically and can be used as chaotic generator in a synchronization-based communication scheme, either stand alone or cascaded with an order three *IIR* filter as shown in Fig.1.

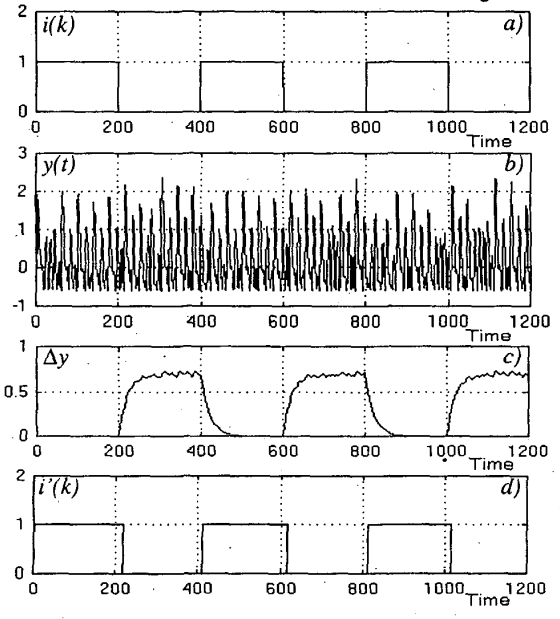

Fig.4 Waveforms of the transmitted information signal *a)*, the transmitted chaotic signal *b)*, the error signal at the receiver *c)*, and the recovered signal *d)*

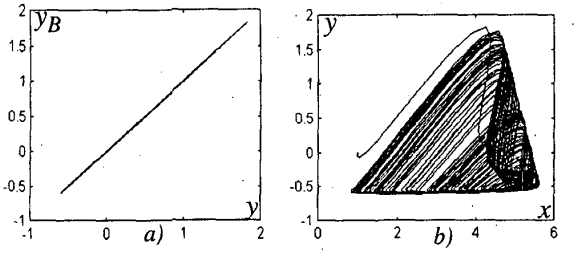

Fig.5 Chaotic synchronization of the transmitter and the receiver *a)* and state space trajectory projection on the plane y-x at the transmitter *b)*

IV. Practical Considerations and Simulation Results

We first discuss some issues related to the level of security offered by our *CC* system. A comparison (in terms of power consumption) between the proposed Colpitts oscillator and the chaotic generator based on Chua's circuit [3] is presented. Then, we present a general discussion of the power consumption of the transmitter system. Finally, research directions to further decrease the overall power consumption of the *CC* system are suggested.

A. Security issues

The increased security of our *CC* scheme comes from the fact that information is processed through two different cascaded circuits. To achieve the highest level of security with our *CC* system, one should first choose the coefficients of the *IIR* (which constitute part of the secret keys for the entire communication scheme) following the rules described in [10]. Consequently, the signal at the output of the filter will present good statistical properties. Then, choose the parameter to be switched, the two values of the parameter, and the state variable of the chaotic generator to be transmitted, so as the receiver is able to take the correct decision when a certain symbol is transmitted, while the threshold of the prediction in the cryptanalysis technique in [15] is less than necessary to make that technique successful.

B. Power consumption--simulation results

Since evidence of reliable information transmission via the *CC* scheme was already presented in the previous sections, the objective now is to illustrate the potential advantage (in terms of power consumption) of using the Colpitts oscillator as a chaotic generator in communication schemes.

To see the difference, in terms of power consumption, between the modified Colpitts oscillator and several practical (discrete-component) realizations proposed so far for chaotic generators, we used Hspice to simulate the Chua's circuit implementations proposed in [7], [1] which are widely used in other communication systems [4].

The simulation results are summarized in Table 1. As we can

see, the advantage of the Colpitts oscillator is not only its simplicity, but also the reduced power consumption (more than 100% savings for a supply voltage of ±5 *V*). In addition, its very large bandwidth (typically *GHz*) makes it useful in many communication applications.

Table 1: Comparison of chaotic generators in terms of power consumption

Type of chaotic generator	Models used for components	Voltage supply [*V*]	Average power [*mW*]	$C_1(=C_2)/R_L/R_E/r_1/L$ (parameters for Colpitts)
modified Colpitts (proposed)	2n2222a	±9	30.37	540p/300/5.4k/2/98.5µH
		±5	9.45	540p/176/5.4k/2/98.5µH
	2n2222a	±9	19.48	540p/220/8.4k/2/98.5µH
		±5	5.76	540p/156/8.4k/2/98.5µH
	2n2222a	±9	16.09	540p/225/10k/2/98.5µH
		±5	**4.70**	540p/157/10k/2/98.5µH
Chua's circuit [7] (2 OpAmps)	UA741	±9	35.91	
		±5	11.13	
	TL082	±9	305.09	
		±5	94.94	
	OPA606E	±9	113.99	
		±5	225.50	
Chua's circuit [1] (1 OpAmp+2 diodes)	TL082	±9	152.88	
	2×1N914	±5	47.55	

Decreasing the voltage supply and modifying the component values of the Colpitts oscillator can reduce its power consumption even bellow 1 *mW*. Since the accuracy of these power estimates is strongly dependent on the type of models which are used for OpAmps, these results are meant primarily to serve as a guide and help understanding the implications of choosing a certain chaotic generator.

In what follows, we present our simulation results on the power consumption of the transmitter (Fig.1). The results are summarized in Table 2. The filter and the parallel-series converter were synthesized with Mentor Graphics tools, extracted with lumped capacitances and resistances, and simulated with Hspice (with MOSFET models from MOSIS, technology 1.2 μm). We use a parallel implementation of the *IIR* filter, so we need a parallel-series converter to convert the output of the filter to a serial stream that enters the Colpitts oscillator. The values of the filter coefficients, which ensure the nonlinear behavior of the filter, were chosen as c_1=30, c_2=25, and c_3=10. Additional circuitry (comprising basically the switch implemented with a dedicated switching transistor with minimal additional circuitry) and clock generators are denoted as "Others" in Table 2. As we see, the power consumption of these circuits is negligible.

To show the impact of data on the power consumption of the *IIR* filter, the simulations are performed for three different sequences, namely *counted*, *pseudorandom* (generated with a maximal-length linear feed-back shift register (LFSR)), and *Gray-code*. We note that the filter is the most power consuming part in the transmitter. Also, the difference between the power consumed when a pseudo-random sequence is applied at the primary inputs and that consumed for a Gray-code one is more than 100%. This suggests that *re-encoding* the information at the input of the *IIR* filter, complemented with special low-power filter architectures, can further decrease the total power consumption to values even lower than 1 *mW* for implementations in deep submicron CMOS technologies. This is one of the research directions that we are currently pursuing.

Table 2: Distribution of power consumption among the blocks of the transmitter

Component	Average power [*mW*]
IIR filter	34.96 (*Counted* seq.)
	64.68 (*Pseudo Random* seq.)
	31.40 (*Gray-code* seq.)
Parallel-series convertor	3.80
Colpitts oscillator	4.70 *(bold value in Table 1)*
Others	< 1

To conclude, the power consumption of the main blocks of the proposed *CC* scheme can be further decreased by choosing an ultra low-power BJT and low-power filter architectures, combined with supplementary re-encoding of the information before being applied at the primary inputs of the *IIR* filter.

V. Conclusion

In this paper, we addressed several aspects related to low-power *CC* systems. Based on classical synchronization principle, a novel structure for a *CC* system was proposed. The proposed system is realized by cascading two circuits, namely a nonlinear third order *IIR* filter and a modified Colpitts oscillator. It is shown that the latter behaves chaotically and synchronization can be used to build a complete *CC* scheme. The simplicity, large bandwidth, and low power consumption make the modified Colpitts oscillator a good solution in terms of power consumption, cost, performance, and security. Simulations results show that the idea of low power chaotic circuits is worth to be further investigated.

References

[1] N.J. Corron, D.W. Hahs, 'A New Approach to Communications Using Chaotic Signals', *IEEE Trans. CAS-I*, Vol. 44, No. 5, May 1997.

[2] L.O. Chua, T. Lin, 'Chaos in Digital Filters', *IEEE Trans. CAS*, Vol. 35, No. 6, June 1988.

[3] L.O. Chua, L. Kocarev, L.K. Eckert, 'Experimental Chaos Synchronization in Chua's Circuit', *Int. J. Bifurcation and Chaos*, Vol. 2, No. 3, 1992.

[4] K.S. Halle, C.W. Wu, M. Itoh, L.O. Chua, 'Spread Spectrum Communication through Modulation of Chaos', *Int. J. Bifurcation and Chaos*, Vol. 3, No. 2, 1993.

[5] M. Hasler, 'Synchronization Principles and Applications', in Circuits&Systems, Tutorials, Ed. Chris Toumazou, 1994.

[6] J. Kawata, Y. Nishio, H. Dedieu, A. Ushida, 'Performance Comparison of Communication Systems Using Chaos Synchronization', *ISCAS98*.

[7] M.P. Kennedy, 'Robust op amp realization of Chua's circuit', *Frequenz*, Vol. 46, No. 3-4, Mar.-Apr. 1992.

[8] M.P. Kennedy, 'Chaos in the Colpitts Oscillator', *IEEE Trans. CAS-I*, Vol. 41, No. 11, Nov. 1994.

[9] G. Kolumban, M.P. Kennedy, L.O. Chua, 'The Role of Synchronization in Digital Communications Using Chaos--Part II: Chaotic Modulation and Chaotic Synchronization', *IEEE Trans. CAS-I*, Vol. 45, No. 11, Nov. 1998.

[10] M. Gotz, K. Kelber, W. Schwarz, 'Discrete-Time Chaotic Encryption Systems - Part I: Statistical Design Approach', *IEEE Trans. CAS-I*, Vol. 44, No. 10, Oct. 1997.

[11] G.M. Maggio, O. De Feo, M.P. Kennedy, 'Nonlinear Analysis of the Colpitts Oscillator and Applications to Design', *IEEE Trans. CAS-I*, Vol. 46, No. 9, Sept. 1999.

[12] U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle, A. Shang, 'Transmission of Digital Signals by Chaotic Synchronization', *Int. J. Bifurcation and Chaos*, Vol. 2, No. 4, 1992.

[13] L.M. Pecora, T.L. Carroll, 'Synchronization in Chaotic Systems', *Phys. Rev. Lett.*, Vol. 64, No. 8, Feb. 1990.

[14] J.G. Proakis, M. Salehi, Communication System Engineering, Prentice-Hall Inc., 1994.

[15] K.M. Short, 'Signal Extraction from Chaotic Communications', *Int. J. Bifurcation and Chaos*, Vol. 7, No. 7, 1997.