Reason - A Technical Magazine
Vol. – IX, 2009 & 2010

SECURE COMMUNICATION SYSTEM USING CHAOS VIA PHASE SHIFT KEYING

Krishnendu Chakrabarty
Principal, Kalyani Government Engineering College, Kalyani-741235

Abstract : A secure communication scheme using chaos and phase shift keying (PSK) has been investigated. A DC-DC converter has been used as a chaos generator.

Keywords : Phase shift keying, Chaos, synchronization.

1. Introduction

A. *Dynamical system and Chaos :*

Matter exists in motion. In fact, matter can not be conceived without reference to its state of motion. There is nothing static or unchangeable in this material world. The things that appear to be static, like the mighty mountains or the stars in the sky, are also changing. Only their rate of change is too slow to be observed in a human lifetime.

Ever since man recognized this fact, the study of dynamics has been a major pursuit. Initially the investigations were piecemeal: Newtonian scientists were studying the dynamics of moving bodies, chemists were studying the changes of chemical properties of matter, and biologists were probing the changes in living organisms. Slowly it came to be recognized that though the objects of study in various disciplines are different, there is an element of commonness in all changes. A body of knowledge gradually emerged, which deals with dynamical systems in general.

Any system whose status changes with time is called a dynamical system. This does not refer only to moving systems; any sort of change in a system comes under the purview of dynamics. The change in chemical composition of a solution is also a problem of dynamics; electronic circuits with no moving parts are also dynamical.

Dynamical systems divide into two major classes :

(1) Those in which time varies continuously that are usually governed by an Ode or PDE and
(2) Those in which time varies discretely that are governed by a DE

The dynamical system is either a state equation of the form

$$\frac{dx}{dt} = \dot{x} = F(x)$$

called an autonomous or unforced ODE and other form $\dot{x} = F(x,t)$, called an non autonomous or forced ODE.

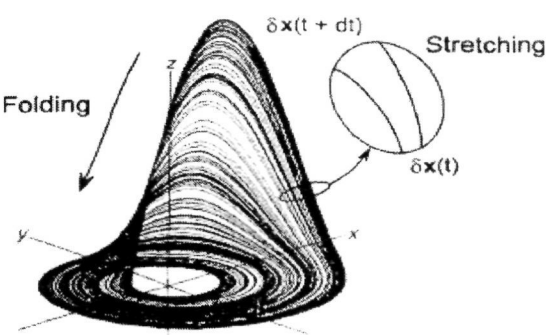
If the system is a discrete equation (DE), the equations are of the form

$x_{n+1} = \Phi(x_n)$ (autonomous) and

$x_{n+1} = \Phi(x_n, t_n)$ (non autonomous)

The former class of dynamical system would be associated with analog circuit while the latter class would be associated with digital circuits. One of the most well-known and potentially useful nonlinear dynamical effects is the bounded, random-like behavior called *chaos*. Chaos has been found to occur in a whole myriad of dynamical systems modeling phenomena from astronomy to zoology, and in frequency ranges from base band to optical.

Chaos is aperiodic long term behavior in a dynamic system that exhibits sensitive dependence on initial conditions.



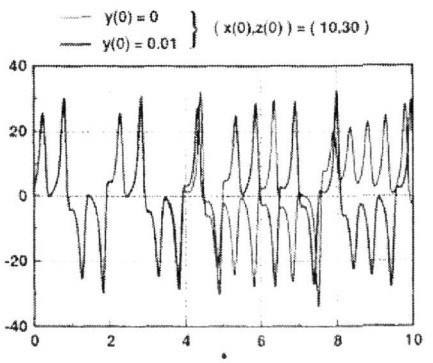


Figure 1

Some characteristic features of chaotic behaviors are shown in the figure1. It provides two such continuous systems. The first figure depicts what is called a strange attractor- a primary manifestation of chaotic behavior in a prototypical third order dynamical system known as Rossler system. The next figure illustrates the sensitivity to initial conditions for another prototypical third order chaotic system called the Lorentz system. The equations of Lorentz system are:

$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = Rx - y - xz$$
$$\dot{z} = -Bz - xy$$

where the physical parameters $\sigma, B \& R$ take on the value 10, 8/3 and 28 respectively. And initial conditions are shown in figure.

The example of dynamical system known as *logistic* map used to model population dynamics is given by $x_{n+1} = \mu x_n (1 - x_n)$, where the parameter μ varies in the interval [0, 4] .This example also serves to illustrate the fundamental concept of bifurcation (Figure:2).

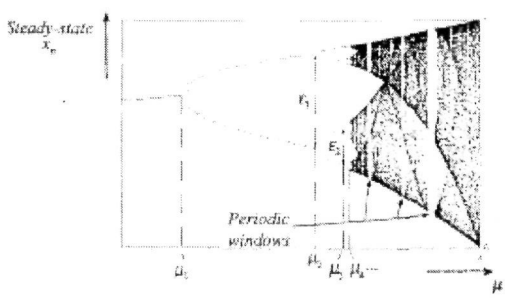


Figure 2

B. *Secure Communication :*

Recently secure communication using chaos has become very popular. This is due to the fact that a chaotic signal is inherently non-periodic and as such possesses continuous spectra. Moreover chaotic signals have a complex structure and are very irregular. One chaos generator will produce a totally different trajectory if it is slightly disturbed in its initial conditions. This makes it difficult to guess the structure of the generator and to predict the signals over longer time. Highly complex and hard to predict signals are classically used to in cryptographic application. The theoretical background of the secure communication originates from the chaos synchronization concept proposed by Precora & Corroll [1,2]

The basic idea is as follows:

- The signal to be transmitted is masked with chaos modulation at the transmitter side.
- By using the so called chaos synchronization, one can recover the signal at the receiver side by various operations [3, 4].

There are many methods of secure communication with chaos are available [5, 6, 7] But these methods suffer from drawbacks. In those cases the synchronization fails with the increase of the strength of the signal to be transmitted. Other methods of secure communication deal with analog signals. But modern communication system is based on digital communication for better performance. Hence in this work a method of secure communication with digital signals based on phase shift keying has been described. Phase modulation helps the system to be robust against contamination of noise in the process of transmission. Moreover the chaos generator used in this work is robust in the sense of synchronization as it does not depend on the strength of the signal.

2. The Scheme

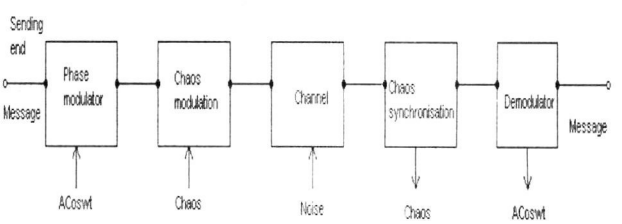


Figure 3

The stream of binary signal that to be transmitted are modulated using phase shift keying (PSK). The PSK signal can be generated by applying the incoming binary data to a phase modulator.

In a PSK system, a sinusoidal carrier wave of fixed amplitude and fixed frequency f_c is used to represent both symbols 1 and 0, except that the carrier phase of each signal differs by a phase of 180^0. The binary PSK signal can be written as

$$s(t) = ACos(2\pi f_c t) - - - - - symbol1$$

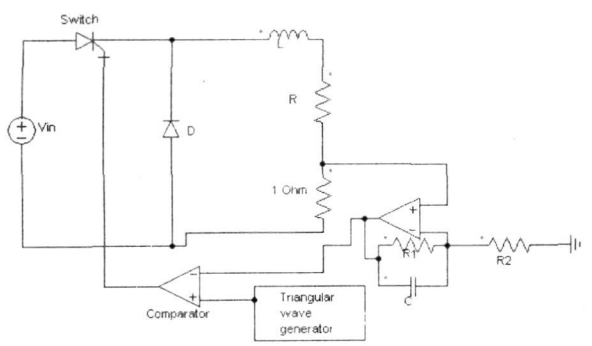
$$s(t) = ACos(2\pi f_c t + \pi) - - - symbol0$$

As the modulating voltage changes from one level to another, the phase modulator output changes its phase in the corresponding fashion.

The PSK signal then modulated with the out put of a chaos generator. The chaos generator used is a PWM controlled DC-DC converter. The output of the converter is transmitted. At the receiver side the PSK signal is recovered by the process of chaos synchronization. The PSK signal is then demodulated using synchronous or coherent detector.

3. The Chaos Generator

The chaos generator is a DC-DC converter shown in the Figure 4. The dynamics of the chaos generator can be governed by two sets of linear differential equation pertaining to on and off condition of the switch. The nonlinearity in this chaos generator is due to switching nonlinearity. The output of the integrator is compared with a triangular wave. The output of the comparator decides the switching of the switch. The diode D acts as a freewheeling diode in this circuit.



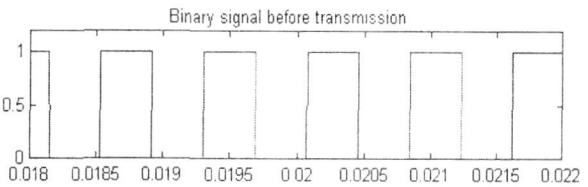
$(R_1 = 10K\Omega, R_2 = 220\Omega, L = 116mH, V_{in} = 20V, R = 25\Omega,$

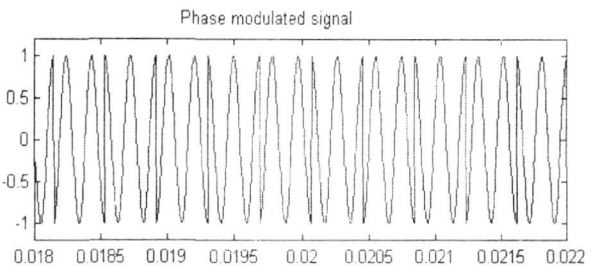
Frequency of triangular wave= $2.55kHz$)

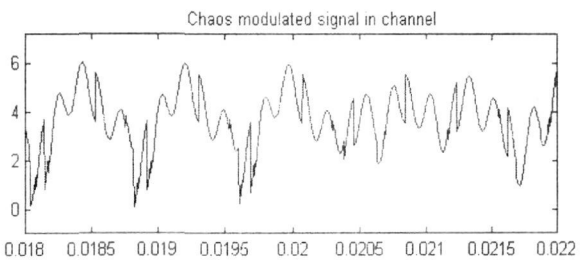
Figure 4

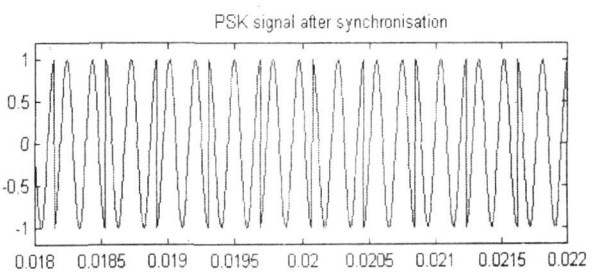
4. Result

The scheme has been implemented by simulation. The figures below show the nature of the signals in the sending end, in the channel and at the receiving end.









5. Conclusion

The secure communication scheme by modulating the PSK modulated signal with chaos has been implemented numerically. The use of DC-DC converter as chaos generator is very useful in the sense of robustness of the synchronization of chaos.

The hardware implementation of the scheme is in progress.

References

[1] Pecora, L.M. and Carroll, T.L., 1990, Synchronisation in chaotic system, Physics Review letter, Vol.64, No.8, pp.821-824.

[2] Pecora, L.M. and Carroll, T.L., 1991, Synchronising chaotic circuits, IEEEE transaction on circuit and systems, Vol.38, No.4, pp.453-456.

[3] Bernardo, M.D., 1996, An adaptive approach to the control & synchronization of continuous time chaotic systems, International Journal of Bifurcation & Chaos, Vol.6, No.3, pp.557-568.

[4] Brucoli,M., Carnimeo, L. and Graggi, G., 1994, A method for the synchronization of chaos using continuous control, International Journal of Bifurcation & Chaos, Vol.4, No.3, pp.483-488.

[5] Lee, C., William, D.B. and Lee, J., 1997, A secure communication system using chaotic switching, International Journal of Bifurcation & Chaos, Vol.7, No.6, pp.1383-1394.

[6] Lipton, J.M. and Dabke, K.P., 1996, Spread spectrum communication based on chaotic system", International Journal of Bifurcation & Chaos, Vol.6, No.12A, pp.2367-2374.

[7] Parlitz, U., Chua, L.O., Kocarev, L., Halle K.S. and Shang, A., 1992, Transmission of digital signal by Chaos synchronization, International Journal of Bifurcation & Chaos, Vol.2, pp.973-977.

Education is not the amount of information that is put into your brain and runs riot there, and undigested all your life. We must have life-building, man-making, character-making assimilation of ideas. If you have assimilated five ideas and made them your life and character, you have more education than any man who has got by Heart a whole library.

– Swami Vivekananda