Simulation Model on Chaotic Asynchronous Transmitter and Receiver

Yilan Zhu
Electrical & Computer Engineering and Computer Science
University of New Haven
West Haven, Connecticut
Yzhu2@unh.newhaven.edu

Andrew Fish, PhD
Electrical & Computer Engineering and Computer Science
University of New Haven
West Haven, Connecticut
AFish@newhaven.edu

***Abstract*— In this research project a new method for secure information transmission, a chaotic communication system, is designed and presented. The architecture of the communication system is constructed using Rössler's attractor of three differential equations for a transmitter and the receiver. The information to be transmitted is concealed in the solutions of Rössler's equations. This allows for the secure transmission of the information. These solutions, together with the message, are then transmitted to a receiver designed to extract the embedded information from the transmitted Rössler's solutions. Simulation results demonstrate the proof of concept of secure transmissions via this method.**

Keywords—communication system, Rössler's attractor, secure transmission

I. Introduction

Network users have become critically concerned about security levels of information systems wiring up their electronic devices, due to the rapid increase of values of their transactions and communication. Security is now playing an essential role in the growth of electronic businesses and the functioning of the whole economy. In fact, according to statistics research by Ponemon Institute LLC [1], more than 43% of companies experienced data breach in 2013. This resulted in a tremendous economic loss for individuals and corporations.

Information security issues encouraged researchers to seek means of data transmission with higher security levels, and they turned to chaos theory. Being one of the three greatest scientific revolution on the 20th century [2], chaos theory was a study of non-linear complex, dynamic systems. The basic principle of chaos theory is that even in an entirely deterministic system, the slightest change in the initial data can cause abrupt and seemingly random change in the outcomes.

Development breakthroughs in chaos theory such as Chua's Circuit (1983), a simple electronic circuit that exhibits classic chaos signal, and the realization of a synchronized coupled system in 1990 by Louis M. Pecora and Thomas L. Carroll, marked great milestones in the development of chaos theory. Many heads were turned for the synchronization of chaos, which could be applied to transmitting information signals in a secure design, developing a new branch of chaos theory, chaos communication. Since then, chaos theory has been playing a significant role for transmitting secure information signals.

II. Methodology

A. Chaos Communication System

Chaos communication, a branch application of chaos theory, was aimed to provide security in information transmission.

Chaos signals, used as a carrier waveform for information transmission, holds unique features for encrypting data signals for the transmission process, including complex behavior, noise-like dynamics (pseudorandom noise) and spread spectrum [3]. These characteristics make chaotic signal an ideal carrier for data transmission.

The type of chaos secure communication method used in this study is chaos masking, where the secure information is being transmitted by adding onto the chaotic signal directly [4]. To avoid the information being destroyed by the disturbance of the chaotic carrier waveform, and to be detectable, the amplitude of the information being sent out should be considered.

In order to implement chaos communications by making the most of such properties of chaos, two chaotic oscillators are required, one as a transmitter and the other as a receiver. At the transmitter terminal, a message signal is modulated onto a chaotic waveform carrier signal before sending out. Once the synchronized receiving oscillator has received the chaotic carrier loaded with information, the message can be decoded and recovered. The following block diagram illustrates an overview of how the chaos communication system is constructed.

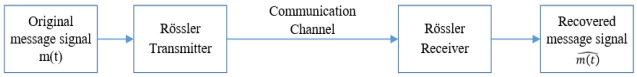

Fig. 1. Overview block diagram of chaotic communication system

B. The Rössler Transmitter

The Rössler transmitter system can be expressed as:

$$\dot{x} = -y - z$$
$$\dot{y} = x + ay$$
$$\dot{z} = b + z(x - c) + m(t)$$

Where m(t) is the message to be transmitted.

The basic idea of the communication system is based on chaotic signal masking and recovery. At the transmitter, the message m(t) is added to the solutions to the Rössler equations, and at the receiver the message is recovered. The Rössler Transmitter could be expressed as:

$$\dot{X} = AX + f(X) + Lm(t) \quad (1)$$

$$\text{Where X} = \begin{bmatrix} x_t \\ y_t \\ z_t \end{bmatrix} \quad (2)$$

$$A_t = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ 0 & 0 & -5.7 \end{bmatrix} \quad (3)$$

$$f(X) = \begin{bmatrix} 0 \\ 0 \\ x_t z_t + 0.2 \end{bmatrix} \quad (4)$$

$$L = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad (5)$$

m(t) = 10sin(1000t) is signal message added into the transmitter. The plot of the Rössler transmitter solutions, which is generated using the 4th order Runge-Kutta integration routine, without m(t) with an initial value of $\begin{bmatrix} x_t(0) \\ y_t(0) \\ z_t(0) \end{bmatrix} = \begin{bmatrix} 10 \\ 10 \\ 10 \end{bmatrix}$, integration step of h = 0.01, and $t \in [0,100]$ is shown in Fig 2.

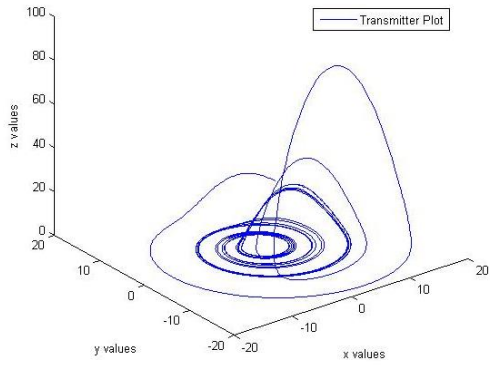

Fig. 2 Plot for Rössler transmitter solutions without implemented m(t)

The plot of the Rössler transmitter with $m(t) = 10sin(1000t)$ embedded is shown in Fig 3. with an initial value of $\begin{bmatrix} x_t(0) \\ y_t(0) \\ z_t(0) \end{bmatrix} = \begin{bmatrix} 10 \\ 10 \\ 10 \end{bmatrix}$, integration step of h = 0.01, and $t \in [0,100]$.

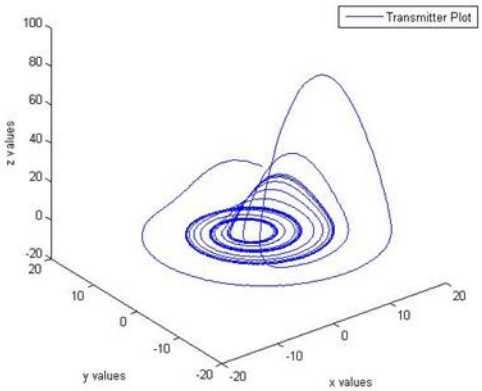

Fig. 3 Plot for Rössler transmitter solutions with implemented m(t)

C. The Rössler Receiver

The Rössler Receiver can be expressed as:

$$\dot{Y} = A_t Y + f(e, X) \quad (8)$$

$$\text{Where Y} = \begin{bmatrix} e_x \\ e_y \\ e_z \end{bmatrix} \quad (9)$$

$$A_r = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ k1 & k2 & k3 - 5.7 \end{bmatrix} \quad (10)$$

$$f(e, X) = \begin{bmatrix} 0 \\ 0 \\ e_x e_z + e_x z_t + x_t e_z \end{bmatrix} \quad (11)$$

$$\widetilde{m(t)} = k_1 e_x + k_2 e_y + (k_3 - 5.7) e_z + e_x e_z + e_x z_t + x_t e_z - \frac{de_z}{dt} \quad (12)$$

where $\widetilde{m(t)}$ is the estimate of the transmitted message m(t), k1, k2 and k3 are parameters chosen to force $Y \to 0$.

The receiver is stabilized [6] by setting the eigenvalues of

$$\begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ k1 & k2 & k3 - 5.7 \end{bmatrix} \text{ to } \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} -1 \\ -2 \\ -3 \end{bmatrix}.$$

This is achieved by setting k1=11.24,k2= 2.408 and k3 = -6.2.

The plot in Fig. 4 is the Rössler Receiver without the message signal, h=0.01, and with an initial condition of (0, 0, 0.2).

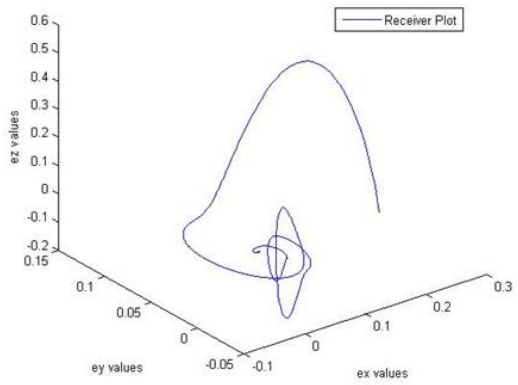

Fig. 4 Plot of Rössler Receiver without m(t)

The plot in Fig. 5 is the Rössler Receiver with the message signal $m(t) = 10\ sin(1000t)$, h=0.01, and with an initial condition of (0, 0, 0.2).

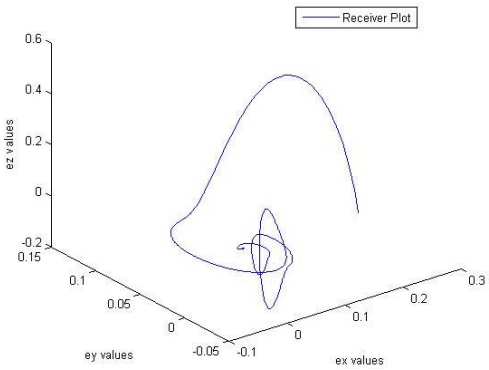

Fig. 5 Plot of Rössler Receiver embedded with m(t)

III. RECOVERY OF ORIGINAL MESSAGE SIGNAL

As mentioned above, $\widetilde{m(t)} = k_1 e_x + k_2 e_y + (k_3 - 5.7)e_z + e_x e_z + e_x z_t + x_t e_z - \frac{de_z}{dt}$,

if $\begin{bmatrix} e_x \\ e_y \\ e_z \end{bmatrix} \to \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $\widetilde{m(t)} \to m(t) = 10\sin(1000t)$.

The plot in **Fig. 8** shows the recovered $\widetilde{m(t)}$.

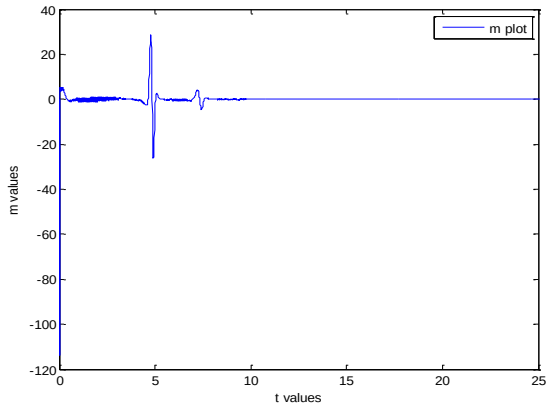

Fig. 8 Recovered message signal $\widetilde{m(t)}$ of time period [0,25]

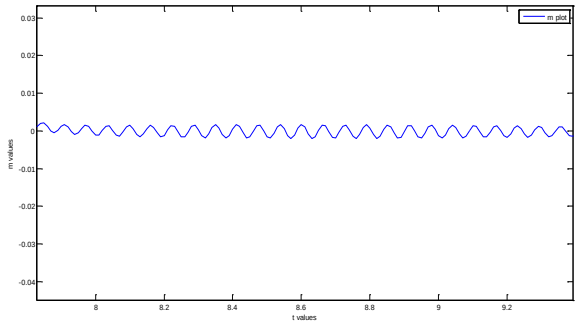

Fig. 9 Recovered message signal (m(t))˜of time period [7.8, 9.4]

In the above demonstrated simulation, the initial values of the receiver is chosen as (0.2,0,0), with the time step h =0.01 results of the recovered information signal m(t), the sine wave could be regenerated.

IV. CONLCUSIONS

The simulations presented above demonstrates a proof of concept of a communication method using the Rössler equations to secure message transmission by embedding a message into a chaotic system. The message itself can be encrypted, further security the information transmission.

REFERENCES

[1] Is Your Company Ready for a Big Data Breach? -The Second Annual Study on Data Breach Preparedness. Ponemon Institute LLC, Traverse City, MI, September 2014.

[2] Greg Frost. (April 30, 2008). MIT Tech Talk (Volume 52, Number 24)

[3] JA Sheikh. (2012). Chaotic Single Generator, P. G. Department of Electronics & IT.

[4] Shen Li-Qun, Ma Jian-Wei, "Adaptive Sliding Mode Synchronization of a Class of Chaotic Systems and its Application in Secure Communication", Xi'an, China, Control Conference (CCC), 2013 32nd (Chinese)

[5] Nikolaos S. Christodoulou (2009), "An Algorithm Using Runge-Kutta Methods of Orders 4 and 5 for Systems of ODEs", International Journal of Numerical Methods and Applications, Volume 2 Number 1, Pages 47-57

[6] Andrew J. Fish Jr, "A Method for Determining the Stability of a Class of Autonomous Nonlinear Continuous Chaotic Dynamical Systems", Control and Decision Conference (CCDC), 2011 (Chinese), Mianyang, China

[7] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.