MATLAB Simulation Model on Chaotic Asynchronous Transmitter and Receiver

Yilan Zhu
Electrical Engineering
Faculty Mentor: Dr. Andrew Fish

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 a Rössler Transmitter and Receiver. A message signal embedded in the transmitter and could be extracted by a stabilized Rössler Receiver.

1. 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 20^{th} 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.

2. Chaos communications 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 in 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

3. Methodology

- **The Rössler system**

The chaos model that would be used in this project would be an elegant, relatively simple three-dimensional chaotic system: the Rössler system, which could be demonstrated with a set of three non-linear ordinary differential equations as follow:

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \qquad (1)$$

Here, $\begin{bmatrix} x1 \\ x2 \\ x3 \end{bmatrix} \in \mathbb{R}^3$ are dynamical variables defining the phase space and a,b and c are parameters, where the values are defined as a=b=0.2 and c=5.7, the most commonly used parameters for Rössler system.

- **The 4^{th} Order Runge-Kutta Method**

In order to simulate the chaotic system in MATLAB, solutions to the above mentioned Rössler system would be necessary. Thus the 4th order Runge-Kutta method was utilized to provide numerical solutions for the Rössler differential equations, as they do not have exact solutions as ordinary differential equations do [5].

- **Rössler Transmitter and Receiver**

The basic idea of the communication system is based on chaotic signal masking and recovery. At the transmitter, a chaotic signal is added to the information signal m(t), and at the receiver the chaotic noise is being removed.

The Rössler Transmitter could be described as

$$\dot{X} = AX + f(X) + Lm(t) \quad (2)$$

where the state vector $X = \begin{bmatrix} x_t \\ y_t \\ z_t \end{bmatrix}$, (3)

$$A = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ 0 & 0 & -5.7 \end{bmatrix}, \quad (4)$$

$$f(X) = \begin{bmatrix} 0 \\ 0 \\ x_t z_t + 0.2 \end{bmatrix}, \quad (5)$$

$$L = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \quad (6)$$

$$\mathrm{m(t)} = 10\sin(\mathrm{t}) \quad (7)$$

m(t) is signal message added into the transmitter. The plot below illustrates the Rössler Transmitter with the m(t) being implemented, an initial value of (10, 10, 10) of a time step h=0.01 over a time frame of [0,100].

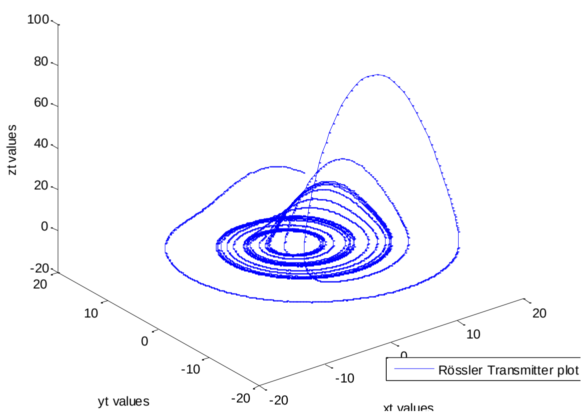

Fig. 2 Plot for transmitter system with implemented message

The Rössler Receiver could be described as

$$\dot{Y} = A'Y + f(Y) + L\widehat{m(t)} \quad (8)$$

where the state vector $Y = \begin{bmatrix} x_r \\ y_r \\ z_r \end{bmatrix}$, (9)

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

$$f(Y) = \begin{bmatrix} 0 \\ 0 \\ x_r z_r + 0.2 \end{bmatrix}, \quad (11)$$

$$L = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad (12)$$

$$\widehat{m(t)} = x_r z_t + x_t z_r - x_r z_r \quad (13)$$

$\widehat{m(t)}$ is the estimate of the input message signal m(t). k1, k2 and k3 are parameters added to the Receiver to stabilize the system. The values of the added k1, k2 and k3 could be determined to stabilize the Rössler Receiver by setting the eigenvalues of $\begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ k1 & k2 & k3 - 5.7 \end{bmatrix}$ to the left half plane [6].

The calculated results for k1, k2 and k3 would be k1= 11.24, k2= 2.408, k3=-6.2. The plot below demonstrated the stabilized Rössler Receiver in its three corresponding state variables x_r, y_r and z_r. As a result of being a stabilized dynamic chaos system, the state variable would gradually going to zero. All the plots demonstrated below is generated under the conditions of a time step h=0.01 together with an initial conditions of (10, 10, 10).

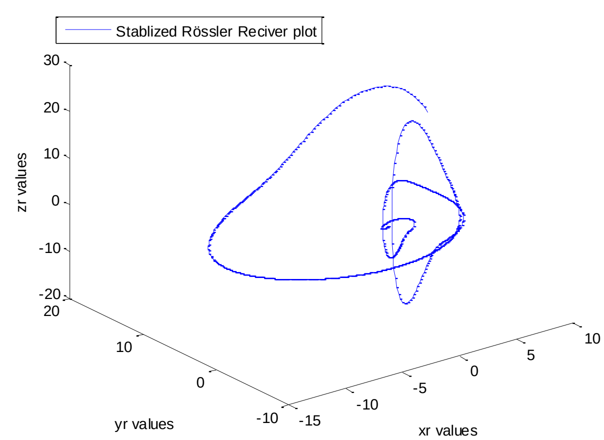

Fig. 3 3D Plot for stabilized Receiver system

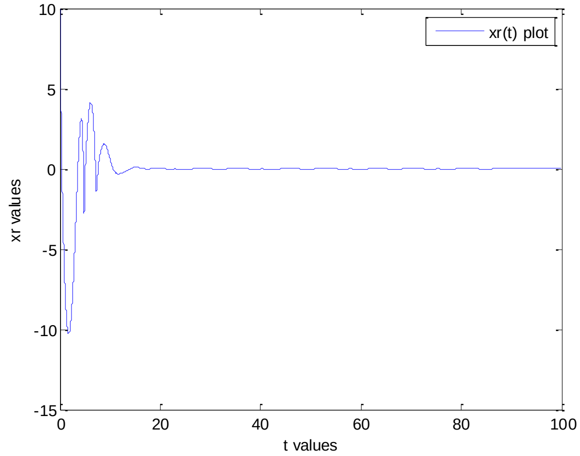

Fig. 4 Plot of x_r of stabilized Rössler Receiver system

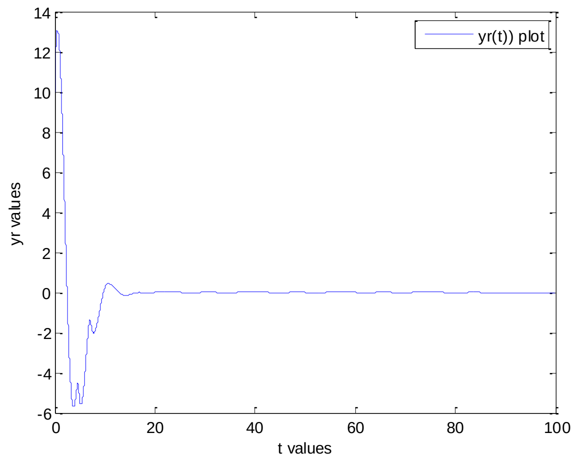

Fig. 5 Plot of y_r of stabilized Rössler Receiver system

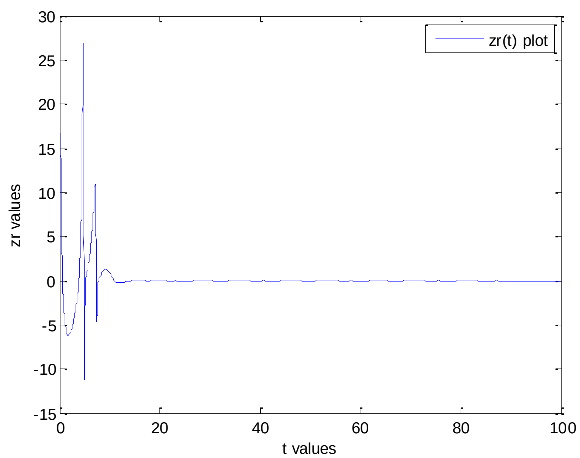

Fig. 6 Plot of z_r of stabilized Rössler Receiver system

In our system, the basic idea is to regenerate the message signal by restating the error system, which is the received signal at the receiver and subtract the transmitted signal to recover m(t). This goal can be achieved as long as the Rössler Receiver could be stabilized. The below graph illustrates the approach to recover m(t).

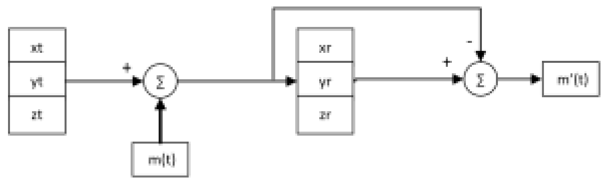

Fig 7. Rössler communication system with system state variables

- **Recovery of the message signal**

As mentioned above, once the Rössler Receiver could be stabilized, the message signal could be recovered. Based on equations (8) - (13), the estimated $\widehat{m(t)}$ could be expressed in state variables of the Rössler Transmitter and Receiver:

$$\widehat{m(t)} = z_r^{\cdot} - \mathrm{k1}x_r - \mathrm{k2}y_r - (\mathrm{k3} - 5.7)z_r - x_r z_r + x_t z_t + x_r z_r \qquad (14)$$

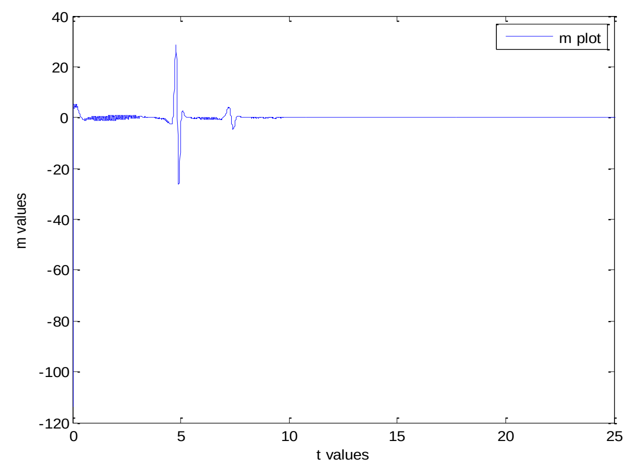

Fig. 8 Recovered message signal m(t) of time period [0,25]

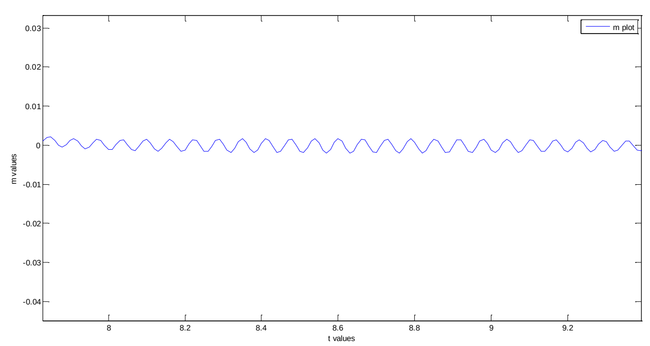

Fig. 9 Recovered message signal m(t) of time period [0, 9.4]

In the simulation, the initial values of the error system 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.

4. Conclusion

A chaos synchronization and secure communication method is designed and displayed. Using the Rössler communication system the communication effectiveness of the communication system is proved. The implemented message signal could be recovered after being embedded into the chaotic transmitter and stabilizing the error system with eigenvalues near the origins of value 1, 2 and 3. This new way of information transmission could benefit the improvement of secure communication.

5. Reference

1. 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

6. Acknowledgements

Yilan Zhu would like to send acknowledgements to Dr. Andrew Fish for being the faculty mentor for this project, providing her with immense guidance on this project. She would also like to thank the University of New Haven Undergraduate Research Fellowship for providing her with a great opportunity to conduct her research. Yilan would also be grateful to the 17th Yale Adaptive and Learning System Workshop for the insights on control system relating to this project.

7. Biography

Yilan Zhu is currently a senior majoring in Electrical Engineering and a minor in Mathematics. She is also an undergraduate peer tutor for EACS, Math and Physics courses in the Center of Learning Resources of the University of New Haven.