ANALYSIS AND DESIGN OF A CHAOTIC COMMUNICATION SYSTEM TESTBED

Noah F. Reddell, Thad B. Welch
US Naval Academy
Electrical Engineering Department
Annapolis, MD

Erik M. Bollt
US Naval Academy
Mathematics Department
Annapolis, MD

ABSTRACT

We explore the advantages of designing a communication system based on chaos by using digital signal processing techniques. Existing work developing communication schemes based on chaos has been done on a theoretical basis or in component based electrical circuits that are not as flexible, particularly for research.

Our work takes a unique technological approach towards exploring the benefits of chaos. We use discrete methods to implement chaotic dynamical systems. Most of our current results are from MATLAB simulations, but we are working towards implementing chaos on digital signal processors (DSPs). These high-speed processors can produce a chaotic carrier through software algorithms rather than in an electrical circuit. The use of discrete methods allows for improvement over earlier schemes. We demonstrate a new dual receiver synchronization method that works because we are able to store samples over an entire bit period and then perform an intelligent comparison. Our results show better bit error probability performance in comparison to previously published methods.

1. INTRODUCTION

Chaotic systems are a class of aperiodic deterministic dynamical systems that are sensitive to slight variations in initial condition. A system's sensitive dependence to initial condition results in the problem that the behavior of the system cannot be predicted for a significant period into the future. The state of a system for the next instant is completely deterministic, but in the long run it cannot be calculated with any degree of accuracy.

These systems then produce random-like behavior due to their unpredictability and relatively wide frequency content. We have looked at both the frequency domain and time domain properties of chaotic systems and find that using them for a message carrier could offer several advantages over traditional modulation schemes such as amplitude modulation and frequency modulation. Our goal is to design a system that can camouflage a transmission near the noise floor.

Initially, it seems strange to attempt communication using a chaotic carrier since the state of a chaotic system cannot be accurately predicted. However, a number of chaotic communication schemes have been proven possible and useful based on the property of self-synchronization [1], [2].

Some chaotic systems can be synchronized with an identical system by allowing for some influence between the two. Both systems will remain chaotic, but one locks to the other. Once synchronization has been achieved, information can be sent. A transmitter's output is modified in some way by a message. Since the receiver follows what the transmitter's state should be, it can detect the modification caused by a message and thus extract the information from the chaotic signal. Meanwhile, the transmission will hopefully continue to look like noise to an outside observer.

We present MATLAB simulations for now, but are working towards implementing our system on two Texas Instruments 'C6711 Digital Signal Processors (DSPs) that discretely emulate a chaotic transmitter and receiver. We started our work as a baseband analysis of the classic Lorenz system and expect to try other systems and eventually modulate to an intermediate carrier frequency. The reason for using the DSP platform is the ease of such alterations.

2. SYNCHRONIZED CHAOS

We consider the famous Lorenz System:

\[ \begin{align*}
\dot{x} &= \sigma(y - x), \\
\dot{y} &= r z - y - x z, \\
\dot{z} &= x y - b z. 
\end{align*} \]  

(1)

The parameters \( \sigma, r, \) and \( b \) have been removed from their original context in Lorenz's convection process but they are still significant for our purposes. It turns out that the Lorenz system given above has a dynamic range that is impractical for the Digital-to-Analog and Analog-to-Digital converters (CODECs) on our DSPs. Additionally, the system evolves at a rate that is impractical for the sampling rate of the CODECs. For these reasons, we will use a magnitude and time scaling change of variables. Scaling magnitude by \( \frac{1}{\sigma} \) allows the \( x \) term to be sent to the Digital-to-Analog converter without saturation. A time scale of \( T_s \) allows efficient use of available CODEC bandwidth. These terms will need to be adjusted based on the particular parameters chosen and the time scaling will be dependent on the step size of the differential equation solver.

The uniform scaling is given by the substitution:

\[ \begin{align*}
u &= \frac{x}{A}, \\
v &= \frac{y}{A}, \\
w &= \frac{z}{A}. 
\end{align*} \]  

(2)

The authors would like to thank the USNA Trident Scholar Program and AFCEA for funding. Also, E.M.B. is funded by the NSF DMS-0071314.
Thus, the scaled drive system (transmitter) is:
\[
\begin{align*}
\dot{u} & = T_S \sigma(v - u), \\
\dot{v} & = T_S (ru - v - Auv), \\
\dot{w} & = T_S (Auv - bw).
\end{align*}
\]

2.1. Drive - Response Coupling based on Parameter Set Match or Mismatch

In our discrete scheme, we further an idea initiated by Cuomo, et al. [3]. They sent a binary message by adjusting the \( b \) parameter of the drive system. This adjustment slightly upsets the synchronization between the drive and response systems. The presence or absence of error at the response system could then be used to determine the message bit.

Our new dual synchronizing response system is as follows. We run two response systems in the receiver DSP. One response system parameter set corresponds to a one-bit and the other corresponds to a zero-bit. Both systems attempt to synchronize with the drive system over the entire bit period. Then, the errors experienced by each response system are compared. The system with less error determines the received bit and both response system states are updated to reflect the better match. By taking advantage of the abilities of DSP hardware, we achieve better performance than a discrete version of the system in [3].

Coupling is achieved by sharing the \( u \) term from the drive system with the response system. Notice in eqn. (4) that \( u \) takes the place of \( u \), in the equations for \( \dot{v} \) and \( \dot{w} \). The variable \( u \) is the influence signal. We maintain the same influence configuration as used by Cuomo, et al. and simplify the problem by letting \( \sigma \) and \( r \) be the same in the response systems as the drive system. The transmitter alters the drive system parameter \( b \) based on a message bit. Parameter \( b \) represents the counterpart parameter in the response system. This \( b \) will either be identical or mismatched.

The response system (receiver) is:
\[
\begin{align*}
\dot{u}_r & = T_S \sigma(v_r - u_r), \\
\dot{v}_r & = T_S (ru - v_r - Auv_r), \\
\dot{w}_r & = T_S (Auv_r - bw_r).
\end{align*}
\]

Error terms are used to evaluate coupling:
\[
\begin{align*}
e_u & = (u - u_r), \\
e_v & = (v - v_r), \\
e_w & = (w - w_r).
\end{align*}
\]

Taking the derivative with respect to time yields
\[
\begin{align*}
\dot{e}_u & = (u - u_r), \\
& = T_S \sigma(v - u) - T_S \sigma(v_r - u_r), \\
& = T_S \sigma(e_v - e_v), \\
\dot{e}_v & = (v - v_r), \\
& = T_S (ru - v - Auv - ru + u_r + Auv_r), \\
& = T_S (e_v - Aew), \\
\dot{e}_w & = (w - w_r), \\
& = T_S (Auv - bw - Auv_r + bw_r), \\
& = T_S (Aew - bw + bw_r).
\end{align*}
\]

2.2. Lyapunov Function Analysis

If we can find a Lyapunov function for the error system above, we can show that it approaches zero over time, and thus the two Lorenz systems synchronize [4]. Lyapunov functions generalize the idea of potential energy. Again we follow Cuomo’s lead and use his Lyapunov function as the basis for ours [3].

\[
E(e_u, e_v, e_w) = \frac{1}{2} \left( e_u^2 + e_v^2 + e_w^2 \right).
\]

To show synchronization, we want to find that the function \( E(e_u, e_v, e_w) \) has a long-term negative slope and so error decreases. Taking the derivative with respect to time:

\[
\frac{dE}{dt} = \frac{\partial E}{\partial e_u} \dot{e}_u + \frac{\partial E}{\partial e_v} \dot{e}_v + \frac{\partial E}{\partial e_w} \dot{e}_w
\]

\[
= \frac{e_u \dot{e}_u + e_v \dot{e}_v + e_w \dot{e}_w}{\sigma} + T_S (e_v e_u - e_v^2 - e_v Auv e_w) + Auev e_w - e_w (bw - b \cdot w_r))
\]

If \( b = b_r \) (Parameter Set Match) then,
\[
\frac{dE}{dt} = T_S (e_u e_v - e_u e_v - 2 - b \cdot e_w)
\]

\[
= T_S (e_u e_v - \frac{3}{2} e_v^2 - 2 - b \cdot e_w^2).
\]

Since \( E \) is positive definite and \( \dot{E} \) is negative definite with \( T_S > 0 \), Lyapunov’s theorem implies \( e(t) \) approaches 0 as \( t \to \infty \). Synchronization will therefore occur. This analysis does not indicate how fast it occurs, but experimentation shows it to be fast enough to achieve a working system.

If \( b \neq b_r \) (Parameter Set Mismatch) then,
\[
\frac{dE}{dt} = T_S (e_u e_v - e_u e_v - e_u^2 - e_v (bw - b \cdot w_r))
\]

The derivative above is inconclusive. We are currently working on analysis to optimize the selection of parameter sets including allowing mismatch in the \( \sigma \) and \( r \) parameters as well. This becomes a six dimensional problem and many technical difficulties arise. Solutions of the Lorenz system, for example, diverge if its parameter set is chosen improperly.

2.3. Increasing Bit Energy Difference

We have found that the performance of the system is essentially based on the difference between the energy of a one-bit and the energy of a zero-bit. Let,

\[
E_{\text{diff}} = |E_1 - E_0|.
\]

This energy difference changes for every bit. To improve the system’s error performance when subjected to noise, we wish to maximize the average energy \( E_{\text{diff}} \) over all transmitted bits.

Because the DSP hardware gives us the ability to compare two receiver versions against the received signal, we...
do not have to worry about completely destroying the synchronization by a parameter mismatch which is too large. The parameter matched version will reset the state of both response systems after the bit period. As a result of our system’s ability to move forward with the best fit system, we are able to maintain synchronization with an aggressive parameter mismatch. For now, we have chosen the two values for \( b \) to be \( b(0) = 2.0 \) and \( b(1) = 6.5 \).

3. DEVELOPMENT OF THE DISCRETE CARRIER

The differential equations described above are continuous systems and must be modified to run our discrete hardware. This can be done by using a differential equation solving algorithm. We have chosen to use the Runge-Kutta 4-5 algorithm because it yields accurate results relative to its processing requirements [5]. The chief issue we have faced when transforming the continuous systems to a discrete environment is that of step size.

The transmission system takes one step via the RK-45 algorithm every time the digital-to-analog converter interrupt service routine is called. This rate is fixed at 48kHz by our CODECs. Instead, the system can be sped up or slowed down by adjusting the RK-45 step size or by adjusting the time scale \( T_S \), which are a related pair. To most effectively utilize the available bandwidth of the CODEC without aliasing, we have found that the limiting factor is the step size-T\( S \) pair. This is because taking a step that is too big causes the RK-45 algorithm to fail and the discrete system does not emulate its continuous model. In the end, we have a system that is sampled at a rate greater than what Nyquist would require. We have not yet experimented with discarding unnecessary samples.

4. RESULTS

Figure 1 shows four cases of two drive systems and two response systems. The drive system chooses parameter set A or B based on the message bit. The plots show the drive system and how the response systems (one using set A and one using set B) respond. We desire that a matched set of parameters between the transmitter and receiver causes a quick and tight coupling while a mismatched set leads to a large error.

Figure 2 shows a single bit window used in our dual synchronizing receiver scheme. This particular window is 100 samples long. The influence signal from the transmitter is affected by additive Gaussian noise and the two receiver versions attempt to synchronize to the influence signal. The error squared is plotted below. The sum of squares of the error for both receiver systems is used to determine the best match with the influence signal. This comparison yields the received bit.

Figure 3 shows the bit error probability performance of our system. The bit period is obviously a crucial factor because it affects how much time the two receivers have to synchronize to or diverge from the influence signal. This also directly effects system data rate.

We have discovered, while trying to ascertain the cause of bit errors, that they are largely due to characteristics of the system itself for relatively large \( \frac{\gamma}{\Omega} \). For basic transmission schemes like BPSK, the energy in a bit is always the same and errors occur when the noise energy is large. This is not true for this chaotic scheme. It turns out that the Lorenz system occasionally goes into regions where the power of \( u \) is significantly less than its average. When the bit window corresponds to these regions, the energy in those bits is smaller than expected. Figure 4 shows a histogram of bit energy and noise energy for 200 bit error observations. This system was running with an average \( \frac{\gamma}{\Omega} \) of 29dB. The histograms indicate that the majority of errors occur when the bit energy is small rather than when the noise energy is large.

5. CONCLUSION

Using a discrete processing approach to explore the benefits of chaos has produced many promising results and has opened up several paths of further research. Discretely generating the chaotic waveforms has both helped to streamline development time and improve upon earlier systems. We continue to work towards a system that works effectively with small signal power. We believe that such a system could be useful for camouflaged military wireless communications.

6. REFERENCES


Fig. 1. All possible combinations of bit sent and receiver system, plotted as voltage vs. sample number. (a), transmitter and receiver use parameter set A (b), transmitter uses set A, receiver uses set B, (c), Transmitter uses set B, receiver uses set A (d), transmitter and receiver use parameter set B.

Fig. 2. Receiver evaluation of a particular bit, (a) Influence signal and attempts to synchronize by both receiver systems (Volts vs. Sample Number), (b) Error$^2$ between both receivers and the influence signal (Volts$^2$ vs. Sample Number).

Fig. 3. Bit error probability as a function of the ratio of energy per bit $E_b$ to noise power spectral density $N_0$ for several communications schemes. (a), the asterisks show the performance of our discrete system using parameter modulation techniques with a good parameter set (b), the open squares show the performance of our discrete system using the more conservative parameter mismatch used in [3] (c), the open circles show the performance of the multiple attractor system in [8] (d), the solid line shows results for baseband BPSK for comparison.

Fig. 4. Histograms of (a), bit energy and (b), noise energy for the dual synchronizing response system over 200 errors bits at $\frac{E_b}{N_0} = 20dB$. The average bit energy and average noise energy for all bits is indicated by the dashed line.