A Chaotic Secure Communication Scheme Based on Duffing Oscillators and Frequency Estimation

Mauricio Zapateiro * **Yolanda Vidal** * **Leonardo Acho** *

* *CoDAlab - Control, Dynamics and Applications Group, Departament de Matemtica Aplicada III, Universitat Politècnica de Catalunya-BarcelonaTECH, Comte d'Urgell 187, E08036 Barcelona, Spain (e-mails: [mauricio.zapateiro, yolanda.vidal, leonardo.acho]@upc.edu).*

Abstract: This work presents a new technique to securely transmit and retrieve a message signal via chaotic systems. In our system, a two-valued message signal modulates the frequency of a Duffing oscillator sinusoidal term. An observer is used in the receiver side to retrieve the sinusoidal signal that contains the message and a novel frequency estimator is then used to reproduce an approximated estimation of the message signal. The performance of the system is analyzed by means of numerical simulations performed in Matlab.

1. INTRODUCTION

The possibility of synchronization of two coupled chaotic systems was first shown by Pecora and Carroll [1990]. The idea is to use the output of the driving system to control the response system in such a way that they both oscillate in a synchronized manner. A wide variety of synchronization schemes have been developed since then, from those that assume perfect knowledge of the system to those that account for uncertainties as can be seen in the works by Chua et al. [1993], Feki [2003] and Benitez and Acho [2007], to name a few. This opened the possibility of using the signals generated by chaotic systems as carriers for analog and digital communications. This discovery soon aroused great interest as a potential means for secure communications [Morgul and Feki, 1999, Andrievsky, 2002, Yang, 2004].

Several works can be found in literature about chaotic secure communications. For instance, Wang and Wang [2009] proposed an observer based on parameter modulation theory where the information modulates the parameters of the chaotic system. Wang and Zhang [2006] proposed a chaotic secure communication scheme based on nonlinear autoregressive filter with changeable parameters where the nonlinear filter was used as a chaotic dynamic system. Hua et al. [2005] proposed a unified chaotic system in which the useful information is embodied in the parameter of the chaotic system.

In this paper, we propose a novel chaotic secure communication system. The message signal is coded into two values that modulate the frequency of the sinusoidal term of a Duffing oscillator. As a result, two chaotic-state signals are sent through the channel. In the receiver side, a Lyapunov-based observer is used to retrieve the sinusoidal term of the oscillator based on the two transmitted chaotic states. Finally, this estimated signal is the input to a frequency estimator that retrieves the message signal. Therefore, with this scheme the message signal modulates the frequency of a sinusoidal signal instead of modulating parameters as it is usually done.

One key contribution of this paper is the frequency estimator. Online frequency estimation has been studied extensively due to its applications in engineering. For example, an approach using globally convergent adaptive notch filter design is studied in Hsu et al. [1999], and an alternative method employing adaptive observer design is given in Bobtsov [2008]. In this paper, we propose a new system where Lyapunov theory is invoked to guarantee the stability of the system. This work assumes that the sinusoidal signal is unbiased. An interesting contribution for the biased case is given in Bobtsov [2008].

This paper is structured as follows. The problem statement is presented in Section 2. The complete chaotic secure communication scheme details are presented in Sections 2.1 - 2.3. In order to illustrate the efficiency of the proposed method, in Section 3 numerical simulations are analyzed. Finally, the conclusions are stated in Section 4.

2. PROBLEM STATEMENT

The objective of this work is to send a signal ω between two points in a secure manner. The components of our proposed chaotic secure communication systems are fully explained in the following subsections. A block diagram of the system is shown in Figure 1

⋆ This work has been partially funded by the European Union (European Regional Development Fund) and the Spanish Ministry of Economy and Competitiveness through the research projects DPI2012-32375 and DPI2011-28033-C03-01 and by the Government of Catalonia (Spain) through 2009 SGR 523. M. Zapateiro is also supported by the 'Juan de la Cierva' Fellowship from the Spanish Ministry of Economy and Competitiveness.

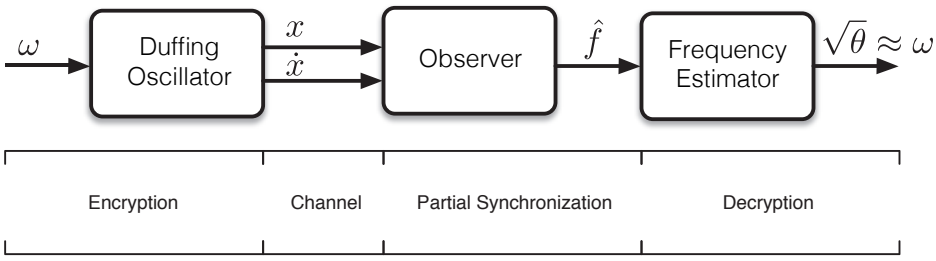

Fig. 1. Block diagram of the proposed method.

2.1 Encryption stage

In the transmitter side of the communication system, there is an encryption system consisting of a Duffing oscillator. A two-valued message signal ω will be used to modulate the frequency of the oscillator sinusoidal term $f(t) = q\cos\omega t$.

The Duffing oscillator is a periodically forced oscillator with nonlinear elasticity and is described by the differential equation

$$\ddot{x} + p_1\dot{x} + p_2x + p_3x^3 = q\cos\omega t$$

where p_1, p_3 and q are positive constants while $p_2 < 0$ and the overdot denotes differentiation with respect to time t. An adequate choice of these parameters leads the oscillator to chaotic behavior.

Let $t = \alpha\tau$, $\alpha > 0$. This time scaling allows for the use of higher frequency values without compromising the chaotic behavior of the oscillator. By defining $\dot{x} = y$ and using the fact that $dt = \alpha d\tau$, we obtain the state space realization of the Duffing oscillator as follows:

$$\dot{x} = \alpha y, \tag{1}$$

$$\dot{y} = \alpha\left(-p_2x - p_3x^3 - p_1y\right) + \underbrace{\alpha q\cos\left(\omega\alpha\tau\right)}_{f(\tau)} \tag{2}$$

where the overdot from now on in the paper denotes differentiation with respect to the new variable τ. Finally, the states x and y that contain the encrypted message are transmitted through the channel.

2.2 Synchronization stage

In the receiver side of the communication system, a partial synchronizer is used to reconstruct the signal f that contains the message signal. It consists of an observer that estimates $\hat{f}$ based on x and y. It is assumed that the signal f, varies slowly with respect to the observer dynamics. That is, we use the hypothesis that $\dot{f} = 0$ to design the observer. However, in practice this hypothesis does not need to be fulfilled as can be seen in Chen et al. [1999, 2000] where by simulation and experiment an observer designed under the same previous assumption can also track fast time-varying disturbances ($\dot{f} \neq 0$). In practice we only need f to vary slowly with respect to the observer dynamics. Thus, the hypothesis used for the observer design is not a restrictive assumption in practice.

Theorem 1. Consider the system

$$\dot{\hat{y}} = k_1(y - \hat{y}) - \alpha(p_2x + p_3x^3 + p_1\dot{x}) + \hat{f}, \quad k_1 > 0 \tag{3}$$

$$\dot{z} = -\hat{y} + y(\alpha p_1k_2 - k_2^2) - k_2z + \alpha k_2(p_3x^3 + p_2x) - \frac{k_2}{\alpha}x, \quad k_2 > 0 \tag{4}$$

where k_1 and k_2 are design parameters and

$$\hat{f} = k_2y + z + \frac{x}{\alpha} \tag{5}$$

Assume that $\dot{f} = 0$. Then:

i) $\hat{f}$ is an observer of the signal f.
ii) $\hat{y}$ is an estimation of y.
iii) $\dot{\hat{y}}$ is an estimation of $\dot{y}$.

Proof 1. Consider the Lyapunov function

$$V = \frac{1}{2}(f - \hat{f})^2 + \frac{1}{2}(y - \hat{y})^2$$

Differentiating the positive definite function V along the system trajectory and taking into account that $\dot{f} = 0$ yield

$$\dot{V} = (f - \hat{f})(-\dot{\hat{f}}) + (y - \hat{y})(\dot{y} - \dot{\hat{y}})$$

and by substituting (3) into the previous equation, we obtain

$$\dot{V} = (f - \hat{f})(-\dot{\hat{f}}) + (y - \hat{y})(\dot{y} - k_1(y - \hat{y}) + \alpha(p_3x^3 + p_2x + p_1y) - \hat{f}) \tag{6}$$

From (2) we have that

$$f = \alpha q\cos\omega\alpha\tau = \dot{y} + \alpha(p_3x^3 + p_2x + p_1y) \tag{7}$$

Substitution of (7) into (6) yields:

$$\dot{V} = (f - \hat{f})(-\dot{\hat{f}} + y - \hat{y}) - k_1(y - \hat{y})^2$$

Clearly, by defining $\dot{\hat{f}}$ as

$$\dot{\hat{f}} = y - \hat{y} + k_2(f - \hat{f}) \tag{8}$$

the derivative of the Lyapunov function becomes

$$\dot{V} = -k_1(y - \hat{y})^2 - k_2(f - \hat{f})^2$$

and, thus $\dot{V}$ is negative definite. To complete the proof of i) and ii) it only remains to prove that the equation (8) corresponds to equations (4) and (5). For this purpose, replace f by $\dot{y} + p_1\dot{x} + p_2x + p_3x^3$ in (8) to obtain

$$\dot{\hat{f}} = y - \hat{y} + k_2(\dot{y} + \alpha(p_1y + p_2x + p_3x^3) - \hat{f})$$

Define $\dot{z} = -\hat{y} + k_2\alpha(p_1\dot{x} + p_2x + p_3x^3) - k_2\hat{f}$. By arranging terms and integrating we obtain

$$\dot{\hat{f}} - y - k_2\dot{y} = \dot{z} \Rightarrow \hat{f} = z + \frac{1}{\alpha}x + k_2y$$

Notice that using the previous equation, $\dot{z}$ can be written as

$$\dot{z} = -\hat{y} + y(\alpha p_1k_2 - k_2^2) - k_2z + \alpha k_2(p_3x^3 + p_2x) - \frac{k_2}{\alpha}x$$

This completes the proof of statements i) and ii). Finally, to prove that $\dot{\hat{y}}$ is an estimation of $\dot{y}$, we can readily see in (3) that $\dot{\hat{y}}$ converges to $\dot{y}$ due to the fact that $\hat{y}$ is an estimation of y and $\hat{f}$ is an estimation of f.

2.3 Decryption stage

The decryption system consists of a novel frequency observer that makes an online estimation θ based on a sinusoidal input with frequency ω. The estimation θ is approximately equal to ω^2.

Theorem 2. Let $r(t) = a\sin\omega t$ be a sinusoidal signal with frequency ω and amplitude a, both unknown. Consider the system

$$\dot{\phi}_1 = \dot{r} - \theta(\phi_1 - \phi_2) \tag{9}$$

$$\dot{\phi}_2 = r - \phi_1 \tag{10}$$

$$\dot{\theta} = \rho\phi_1(\phi_1 - \phi_2) \tag{11}$$

where $\rho > 0$. Then $\sqrt{\theta}$ is an estimation of ω.

Proof 2. We begin the proof by considering the following system,

$$\dot{\phi}_1 = \dot{r} - \theta(\phi_1 - \phi_2) \tag{12}$$

$$\dot{\phi}_2 = r - \phi_1 \tag{13}$$

where $r(t) = a\sin\omega t$. Suppose that there exists $\theta = \theta^*$ such that $\phi_1 = 0$, which implies that $\dot{\phi}_1 = 0$. Then, the system (12)-(13) reduces to

$$\theta^*\phi_2 = -\dot{r} \tag{14}$$

$$\dot{\phi}_2 = r \tag{15}$$

Thus, $\theta^*\dot{\phi}_2 = -\ddot{r}$, which is equivalent to

$$\theta^* r = -\ddot{r} \tag{16}$$

corresponding to a linear oscillator with the oscillation frequency: $\theta^* = \omega^2$. This is because $\ddot{r}(t) = -\omega^2 a\sin\omega t = -\omega^2 r(t)$, i.e. it is equivalent to (16). Now, the objective is to find a dynamic system for θ such that a combination of ϕ_1 and θ yields a stable equilibrium point in the sense of Lyapunov. In order to fulfill this objective, consider the following Lyapunov function:

$$V = \frac{1}{2}\phi_1^2 + \frac{1}{2\rho}(\theta - \theta^*)^2 + \frac{1}{2}\left(\phi_2 - \left(-\frac{\dot{r}}{\theta^*}\right)\right)^2 \tag{17}$$

Here, ρ is a positive constant. The last term in (17) captures the convergence of ϕ_2 to a periodic motion, as expected. Then, the derivative of V along the trajectory of system (12)-(13) is

$$\dot{V} = \phi_1\dot{\phi}_1 + \frac{1}{\rho}(\theta - \theta^*)\dot{\theta} + \left(\frac{\theta^*\phi_2 + \dot{r}}{\theta^*}\right)\left(\dot{\phi}_2 - \left(-\frac{\ddot{r}}{\theta^*}\right)\right)$$

Substitution of (16) into the previous equation yields

$$\dot{V} = \phi_1\dot{r} - \theta\phi_1(\phi_1 - \phi_2) + \frac{1}{\rho}(\theta - \theta^*)\dot{\theta}$$

Defining $\tilde{\theta} = \theta - \theta^*$, and using (14),

$$\begin{aligned}\dot{V} &= -\phi_1\theta^*\phi_2 - \theta\phi_1(\phi_1 - \phi_2) + \frac{1}{\rho}\tilde{\theta}\dot{\theta} \\ &= \tilde{\theta}\left[\frac{\dot{\theta}}{\rho} - \phi_1(\phi_1 - \phi_2)\right] - \theta^*\phi_1^2\end{aligned} \tag{18}$$

Finally, by defining $\dot{\theta}$ as

$$\dot{\theta} = \rho\phi_1(\phi_1 - \phi_2) \tag{19}$$

equation (18) becomes

$$\dot{V} = -\theta^*\phi_1^2$$

Thus, $\dot{V}$ is negative semi-definite. Also, the equations above imply that $\phi_1, \theta, \dot{\phi}_1, \dot{\theta} \in L_\infty$ and $\phi_1 \in L_2$. By Barbalat's lemma we can guarantee that $\dot{V} \to 0$ as $t \to \infty$. Therefore, we can conclude that ϕ_1 converges to zero as time passes. Note this implies that:

(i) θ is an estimation of θ^*. The convergence of ϕ_1 to zero after a period of time implies, using (19), that $\dot{\theta}$ converges to 0 as time passes by. Thus θ converges to a constant value θ^* (as ϕ_1 converges to zero).

(ii) ϕ_2 is bounded. As ϕ_2 converges to zero and θ converges to θ^* then we have that ϕ_2 remains close to $-\frac{\dot{r}}{\theta^*}$ as $t \to \infty$. That is, ϕ_2 converges to a periodic motion. This is verified in the numerical simulations.

Remark 1: In the implementation of our communication system, $r = \hat{f} \approx \alpha q\cos\alpha\omega\tau$ and consequently $\sqrt{\theta} \approx \alpha\omega$.

Remark 2: Note that $\dot{r} = \dot{\hat{f}} = \dot{z} + y + k_2\dot{y}$. However $\dot{y}$ is not available in the receiver side of the communication system but we can appeal to Theorem 1 in order to make $\dot{y} \approx \dot{\hat{y}}$. Thus, it can be rewritten as $\dot{\hat{f}} \approx \dot{z} + y + k_2\dot{\hat{y}}$. This expression is not too appropriate for implementation though. Recall from (4) that $\dot{z}$ contains a cubic term that makes this derivative sensitive to noise or small errors. We propose the use of the following filter which has proven to accurately approximate derivatives. The dynamics of this system is [Spong and Vidyasagar, 1989]:

$$\dot{g} = \left(\hat{f} - g\right)/\beta, \quad \dot{\hat{f}} \approx \left(\hat{f} - g\right)/\beta \tag{20}$$

with $\beta > 0$ and sufficiently small.

Remark 3: The frequency estimator does not require the amplitude of the sinusoid in order to make a correct estimation of its frequency. Thus, we can use as input to the frequency estimator a downscaled version of $\hat{f}$. By doing this, we can avoid high overshoots during the transient and besides it facilitates the physical implementation of the system. Therefore, we use $r = \mu\hat{f}$ and $\dot{r} = \mu\dot{\hat{f}}$, $0 < \mu < 1$.

A block diagram of the frequency estimator (9)-(11) is shown in Figure 2.

3. NUMERICAL SIMULATION

In order to analyze the performance of the chaotic secure communication system, the systems of equations (1)-(2), (3)-(5) and (9)-(11) were implemented and simulated in Matlab with the following parameter values:

- Duffing oscillator: $p_1 = 0.4$, $p_2 = -1.1$, $p_3 = 1$, $q = 2.1$, $\alpha = 5$
- Observer values: $k_1 = k_2 = 400$.
- Frequency estimator values: $\rho = 400$, $\mu = 0.5$
- Initial conditions: $x(0) = 0.1$, $y(0) = -0.1$, $\hat{y}(0) = 0$, $z(0) = 0$, $\phi_1(0) = \phi_2(0) = \theta(0) = 0$, $g(0) = 0$.

The message signal is a sequence of values $\omega = \{1.8, 2.2\}$. The differential equation solver used was the function

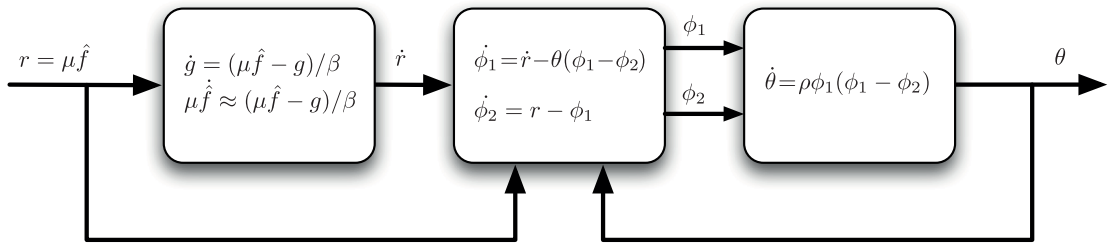

Fig. 2. Block diagram of the proposed frequency estimator.

ode45. Figures 3-5 show the performance of the transmitter side of the chaotic communication system. In these figures we observe a 40-second simulation where a message consisting of two values was sent. Figure 3 shows three signals, namely, the states x and y and the recovered signal $\hat{y}$. As can be seen, there is an accurate match between the sent signal x and its estimate $\hat{y}$ as predicted by Theorem 1. A zoomed area of these signals is shown in Figure 4 where it is possible to see that the observer takes less than 0.01 seconds to synchronize with the transmitter signal. An x versus y plot is shown in Figure 5 where we can see the chaotic behavior of the oscillator during the transmission.

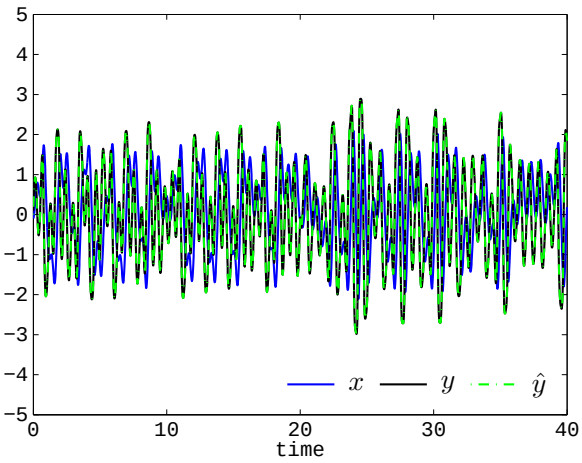

Fig. 3. Transmitter performance. Transmitted states x and y and estimation $\hat{y}$.

Figures 6-8 show the performance of the receiver side of the system. Figure 6 compares the sinusoidal signal $f = \alpha q \cos \omega \alpha \tau$ and the signal retrieved by the observer in the receiver side $\hat{f}$. In the zoomed area shown in Figure 7 we can see that the observer takes 0.01 seconds approximately to estimate the oscillator sinusoidal signal from the transmitted oscillator states. Finally, Figure 8 compares the retrieved confidential message with the original sent message.

Figure 9 is an analysis of the different values of the scaling factor μ. During this simulation, the parameters k_1, k_2 and ρ remained the same as those presented at the beginning of this section. Thus, the effect of increasing μ is an overshoot decrease in the frequency estimator response. Moreover, a lower μ implies a longer transient response. On the other hand, Figure 10 depicts the performance of the communication system for different values of α. In this case, there is the need to modify the parameters k_1, k_2

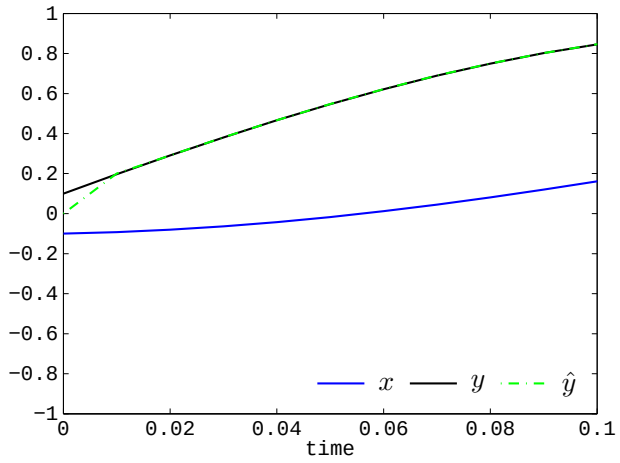

Fig. 4. Transmitter performance. Closer look at the transmitted signals and estimation.

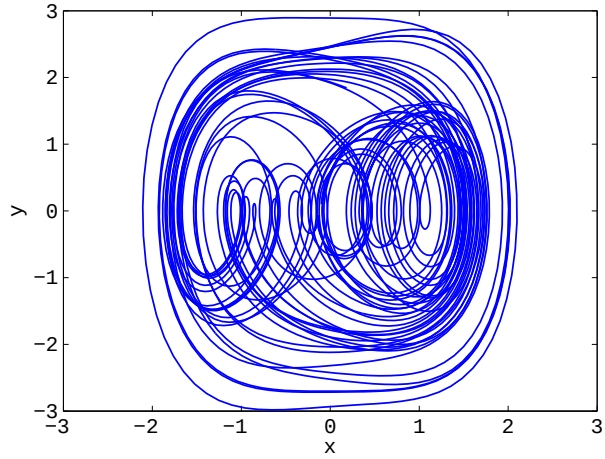

Fig. 5. Transmitter performance. Oscillator chaotic dynamics.

and ρ so that the system performs satisfactorily. Thus, for $\alpha = 1$ we have $k_1 = k_2 = 40$, $\mu = 1$ and $\rho = 100$; for $\alpha = 3$, $\alpha = 5$ and $\alpha = 7$, we have $k_1 = k_2 = 400$, $\mu = 0.5$ while the values of ρ are 900, 250 and 250 respectively. As it can be seen, varying α allow us for controlling the response of the observer, that is, we can make it reduce the oscillations, the time response and the overshoots. Setting an adequate value of α is a compromise among these criteria. Finally, Figure 11 shows the transmitted and retrieved message in a 100-second simulation with $\alpha = 5$, $\mu = 0.5$, $\rho = 250$ and $k_1 = k_2 = 400$.

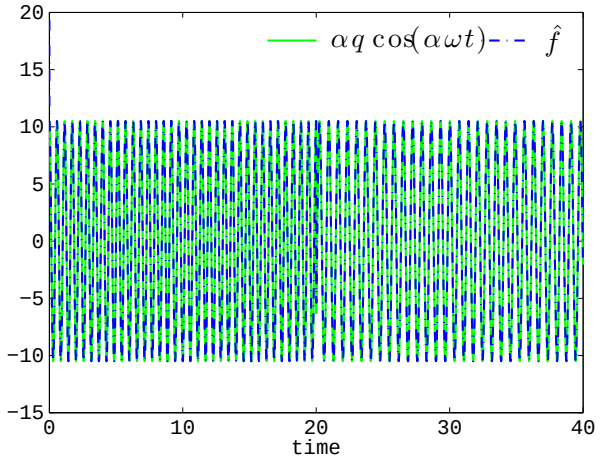

Fig. 6. Receiver performance. Retrieved sinusoidal signal from the observer in the receiver side.

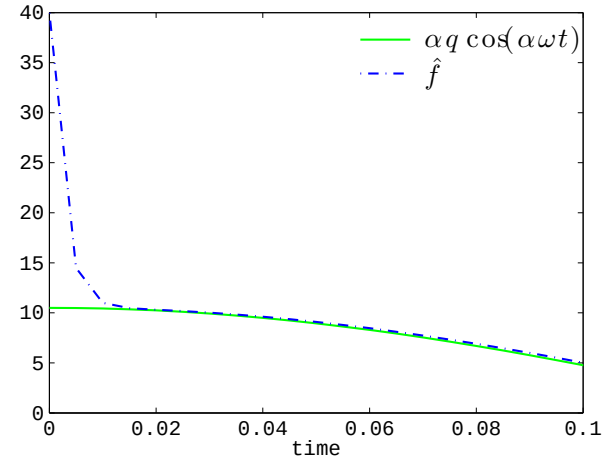

Fig. 7. Receiver performance. Closer look at the retrieved sinusoidal signal.

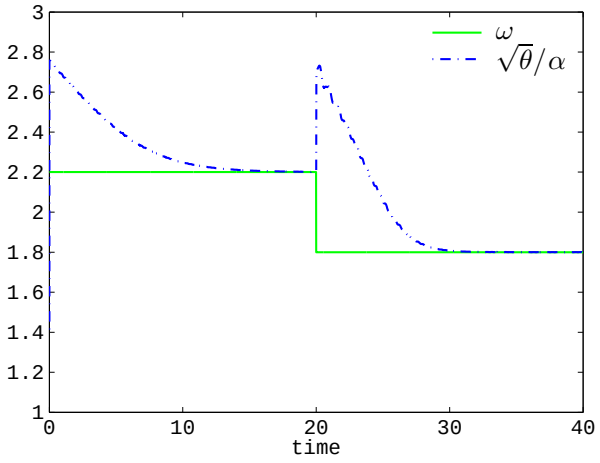

Fig. 8. Receiver performance. Retrieved message.

Finally, the simulations were performed assuming a noisy channel. A second-order Butterworth filter with 40 rad/s cut-off frequency was added in the receiver side so that the

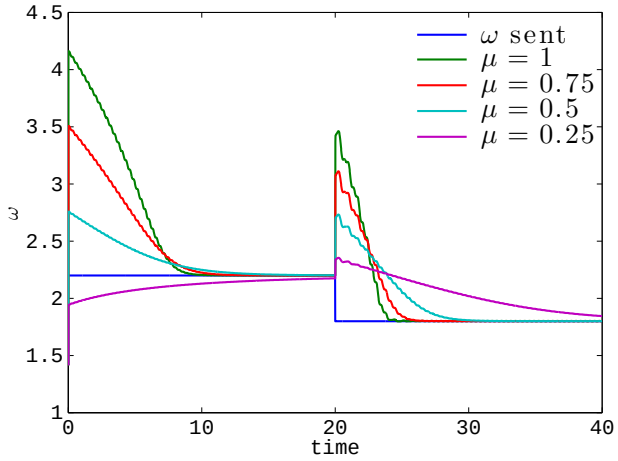

Fig. 9. Effect of varying μ.

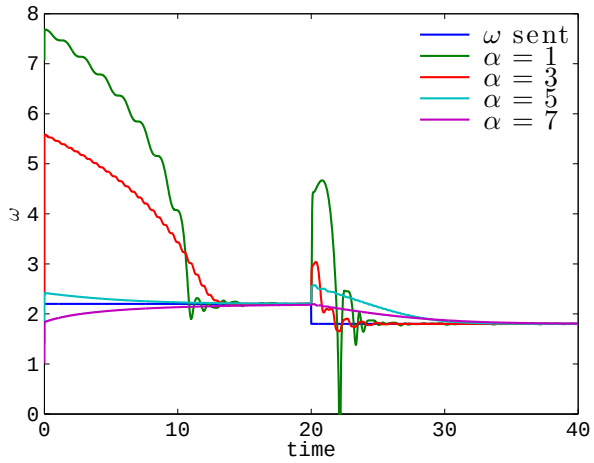

Fig. 10. Effect of varying α.

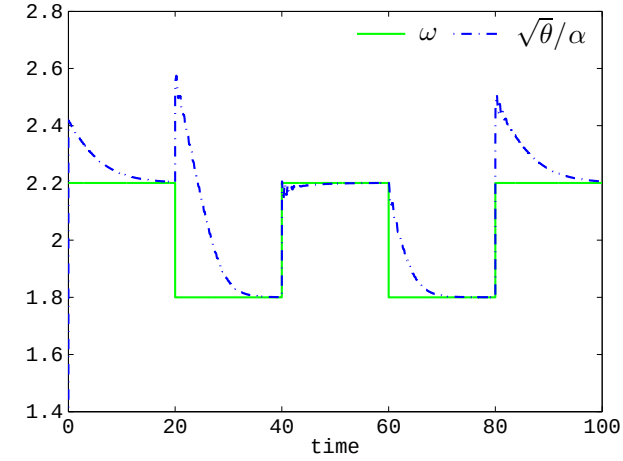

Fig. 11. Transmitted and retrieved messages.

signal states x and y were processed before they entered the observer. The result of the 100-second simulation is shown in Figure 12. The systems proofs to be robust against noise as can be inferred from the accuracy of the message signal estimation. Moreover, note that the

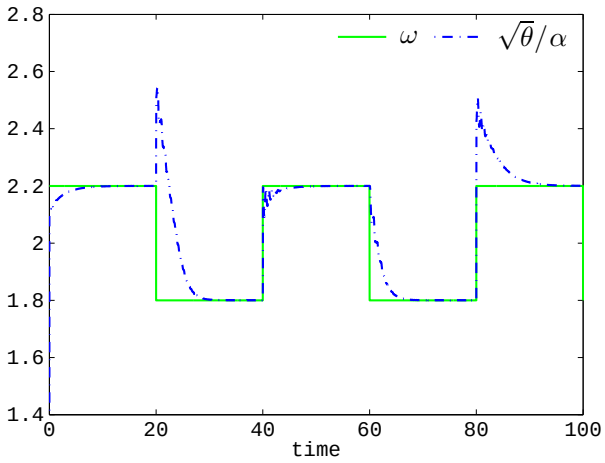

Fig. 12. Transmitted and retrieved messages in a 100-second transmission through a noisy channel.

transient response has lower peaks and faster response in comparison to the case examined earlier where an ideal noiseless channel was considered. This is because the noise filters remove the high frequency contents of the state signals x and y produced by the abrupt changes in the message signal when it enters the oscillator (e.g. from 1.8 to 2.2 and vice versa).

4. CONCLUSION

In this paper we have proposed a new chaotic secure communication scheme with frequency estimation. The message is a two-valued signal which is used as the frequency of oscillation of the Duffing oscillator sinusoidal term. In order to retrieve the message, we use an alternative approach to on-line frequency estimation. This approach was obtained by examining the problem from a novel viewpoint and invoking the Lyapunov theory. A Lyapunov-based observer was formulated for its use in the synchronization of the chaos-based communication system. We introduced a scaling parameter in the Duffing oscillator in order to improve the frequency estimator response performance. Numerical simulations have demonstrated the highly effective performance and robustness of the proposed method.

5. FUTURE WORK

In order to increase the security of the system, we propose the addition of dynamic encryption and decryption functions. Various methods have been proposed to design secure communications based on chaotic signals, where some popular ones are the additive masking and chaotic parametric modulation methods. When one-channel of communication is used for transmitting the information, the secure communication has a low level of security for a smart intruder. According to Jiang [2002], by using two-channels of communication, the system security level is improved. This security level can be further increased if, together with the two-channels of communication, encryption and decryption functions are employed. These functions can be added to our security system in that same way as they are used in Jiang [2002] without altering the proof of all technical details given for our secure system. Moreover, some cryptography algorithms (based on chaotic signals) can be added too if we want to increase more the security level of our system.

REFERENCES

B. Andrievsky. Adaptive synchronization methods for signal transmission on chaotic carriers. *Mathematics and Computers in Simulation*, 58(46):285 – 293, 2002. ISSN 0378-4754. Chaos Synchronization and Control.

Sinuh Benitez and Leonardo Acho. Impulsive synchronization for a new chaotic oscillator. *Int. J. of Bifurcation and Chaos*, 17:617–623, 2007.

A. Bobtsov. New approach to the problem of globally convergent frequency estimator. *Int. J. of Adaptive Control and Signal Processing*, 22:306–317, 2008.

W H Chen, D J Ballance, P J Gawthrop, J Gribble, and J O'Reilly. A nonlinear disturbance observer for two link robotic manipulators. *Proceedings of the 38th IEEE Conference on Decision and Control*, 4:3410–3415, 1999.

W H Chen, D J Ballance, P J Gawthrop, and J O'Reilly. A nonlinear disturbance observer for robotic manipulators. *IEEE Transactions on Industrial Electronics*, 47(4):932–938, 2000.

L. Chua, M. Itoh, L. Kocarev, and K. Eckert. Chaos synchronization in chua's circuit. *J. Circ. Syst. Comput.*, 3:93–108, 1993.

Moez Feki. An adaptive chaos synchronization scheme applied to secuere communication. *Chaos, Solitons and Fractals*, 18:141–148, 2003.

Liu Hsu, R. Ortega, and G. Damm. A globally convergent frequency estimator. *Automatic Control, IEEE Transactions on*, 44(4):698 –713, apr 1999. ISSN 0018-9286. doi: 10.1109/9.754808.

Changchun Hua, Bo Yang, Gaoxiang Ouyang, and Xinping Guan. A new chaotic secure communication scheme. *Physics Letters A*, 342:305–308, 2005.

Zhong-Ping Jiang. A note on chaotic secure communication systems. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, 49(1): 92–96, 2002.

Omer Morgul and Moez Feki. A chaotic masking scheme by using synchronized chaotic systems. *Physics Letters A*, 251(3):169 – 176, 1999. ISSN 0375-9601.

Louis M. Pecora and Thomas L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64:821–824, Feb 1990. doi: 10.1103/PhysRevLett.64.821.

M.W. Spong and M. Vidyasagar. Robot dynamics and control. *John Willey & Sons, Inc*, 1989.

Xiang-Yuan Wang and Ming-Jun Wang. A chaotic secure communication scheme based on observer. *Communications in Nonlinear Science and Numerical Simulation*, 14:1502–1508, 2009.

Xiaomin Wang and Jiashu Zhang. Chaotic secure communication based on nonlinear autoregressive filter with changeable parameters. *Physics Letters A*, 357:323–329, 2006.

Tao Yang. A survey of chaotic secure communication systems. *Int. J. Comp. Cognition*, 2:81–130, 2004.