2010 International Symposium on Nonlinear Theory and its Applications
NOLTA2010, Krakow, Poland, September 5-8, 2010

Application of Open-Plus-Closed-Loop Control to Secure Communications Using Chaos Masking

Yusuke Yoshida and Takaya Miyano

Department of Micro System Technology, Ritsumeikan University,
1-1-1 Noji-Higashi, Kusatsu, Shiga 525-8577, JAPAN
Email: tmiyano@se.ritsumei.ac.jp

Abstract—We have applied the open-plus-closed-loop control method, recently devised by Grosu et al., to secure communications using chaos masking. In our method, a message is treated as part of the parameter mismatch between the chaotic oscillators installed on a drive and a response system. In the drive system, a message is added to the state variable of the chaotic oscillator as dynamical noise and thus the time-integrated message is encrypted by the chaotic signal. In the response system, the message is decrypted by subtracting the chaotic carrying signal reproduced by chaotic synchronization using the open-plus-closed-loop control method from the received signal, followed by differentiation with respect to time. We show our experiment for the encryption and decryption of an actual speech signal to assess the performance of our method.

1. Introduction

Chaos synchronization is one of important discoveries in nonlinear science, which has stimulated the development of applications of chaos [1, 2]. An outstanding example is secure communications using chaos masking, which was discovered by Cuomo, Oppenheim and Strogatz [3, 4]. Their method relies on the fact that a couple of identical chaotic oscillators sharing a particular state variable can synchronize with each other because of negativity of the conditional Lyapunov exponents. It has recently been applied to a commercial communications network system with optical devices as the chaotic oscillators [5]. Advanced analysis concerning chaos-based communications have recently been performed, for instance, in [6, 7]. However, Cuomo-Oppenheim's method has two weak points. One is negativity of the conditional Lyapunov exponent and the other is parameter mismatch between chaotic oscillators that is unavoidable in actual communications systems. Because of negative conditional Lyapunov exponents, which are required for the synchronous state of the oscillators to be dynamically stable, we are obliged to have a narrow choice of the dynamics governing the oscillators and the mode of coupling between the oscillators. This allows eavesdroppers to identify the dynamics. Parameter mismatch causes a technical problem of the need to precisely tune the chaotic oscillators installed on the drive and response systems.

We have recently proposed an alternative method for secure communications using chaos masking that is free from not only the conditional Lyapunov exponent but also the precise tuning of the chaotic oscillators [8]. Our method is based on chaotic synchronization using the open-plus-closed-loop (OPCL) coupling recently devised by Grosu and co-workers [9]–[13]. In our method, a message is treated as part of the parameter mismatch between the chaotic oscillators and added to a state variable of the chaotic oscillator of the drive system as dynamical noise. In this manner, the time-integrated message is encrypted by the chaotic signal. In the response system, the message is retrieved by subtracting the chaotic carrying signal reproduced by the OPCL control method from the received signal, followed by differentiation with respect to time. The parameter mismatch as well as the parameter of the chaotic oscillators are used as the keys to synchronize the chaotic oscillators of the drive and response systems, which may improve the security of communications.

In this paper, we demonstrate our experiment for the secure communications of an actual speech signal to test the utility of our method. In section 2, we provide a short summary of the mathematics of our method. In section 3, we show the procedure and experimental system for our experiment and show results. In sections 4 and 5, we discuss our results and make conclusions.

2. Theory

The main points of the OPCL control method are as follows. For details, see [9, 10]. Let us consider making $y(t) \in R^d$ synchronous with $x(t) \in R^d$ whose time evolutions are governed by $\dot{x} = F(x) + \Delta F(x)$ and $\dot{y} = F(y) + C_1(x) + C_2(x, y)$: $\mid y(t) - x(t) \mid \rightarrow 0$ as $t \rightarrow \infty$. ΔF denotes parameter mismatch. The open-loop coupling C_1 and the closed-loop coupling C_2 are given as $C_1(x) = \dot{x} - F(x)$ and $C_2(x, y) =$

$[H - DF(x)](y - x)$, respectively, where $DF(x)$ is the Jacobian matrix ($\in M_d$) of F evaluated at x and H ($\in M_d$) is a Hurwitz matrix whose eigenvalues have a negative real part. Complete synchronization of y with x is realized when introducing both C_1 and C_2. Let us assume that x is close to y as a consequence of the open-loop coupling C_1. Then, $F(y)$ is written as $F(y) \approx F(x) + DF(x)(y - x)$ using Taylor's expansion and the time evolution of the difference $e = y - x$ is subject to $\dot{e} = H(y - x) = He$. The negative real part of the eigenvalues of H leads to $e \to 0$ as $t \to \infty$, despite the parameter mismatch $\Delta F(x)$. The synchronization of y with x is thus achieved irrespectively of the conditional Lyapunov exponent.

We next show a concrete procedure for our method on the basis of the OPCL control method using chaotic oscillators subject to the Sprott equations [10, 14]. Let us express the state variables of a drive system as x_1, x_2 and $x_3 \in R$ and the corresponding variables of a response system as y_1, y_2 and $y_3 \in R$. A message signal $m(t) \in R$ is encrypted using

$$\dot{x}_1 = -(k + \Delta k)(x_2 + m) \ , \quad (1)$$
$$\dot{x}_2 = x_1 + x_3 \ , \quad (2)$$
$$\dot{x}_3 = x_1 + (x_2 + m)^2 - x_3 \ , \quad (3)$$

where k is a parameter and Δk is parameter mismatch. The message is continuously input into the equations as dynamical noise to x_2 as if m were part of the parameter mismatch. Thus, m is mixed into the carrying signal x_2 and numerically integrated. We make the magnitude of m sufficiently smaller than that of the carrying signal, i.e., $\| m \| \ll \| x_2 \|$, not to seriously deform the message.

The response system receives the x_2 signal that contains the integrated message. The message can be decrypted using

$$\dot{y}_1 = -ky_2 - \Delta k x_2 \ , \quad (4)$$
$$\dot{y}_2 = y_1 + y_3 \ , \quad (5)$$
$$\dot{y}_3 = y_1 + y_2^2 - y_3 - (1 + 2x_2)(y_2 - x_2) \ , \quad (6)$$

where we use the Hurwitz matrix H given in [10].

$$H = \begin{pmatrix} 0 & -k & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix} \quad (7)$$

Because y_2 is synchronized with the chaotic component of the received signal, subtraction of y_2 from x_2 and the subsequent differentiation of $x_2 - y_2$ with respect to time enable the retrieval of the original message m. The parameter mismatch Δk must be exactly known to achieve the synchronization of the chaotic oscillator in the response system with that in the drive system. Accordingly, Δk is a key for decrypting the message.

3. Numerical Experiments

We conducted an experiment to test our idea. In this experiment, a speech signal "Yes, we can." articulated by one of the authors (Y.Y.) was used as a message. Our experimental procedures are as follows. The speech signal was acquired in the WAV format using a microphone of high quality (Shure SM81) and a sound processing system (Yamaha MW8CX) under a sampling frequency of 11.025 [kHz] and a quantization precision of 8 bits. The file format of the message was converted to the TEXT format. Subsequently, the numerical calculation for the encryption and decryption of the message was performed using the method described in the preceding section on a personal computer. The file format of the message after encryption and decryption was again converted to the WAV format. Then, we listened to the original, encrypted and decrypted messages with a speaker system and compared their sound qualities to assess the performance of our method for secure communications.

The parameter and parameter mismatch of the Sprott oscillators were set to $k = 0.225$ and $\Delta k = 0.0225$ (10 % parameter mismatch), respectively. In the encryption and decryption of the message, the fourth-order Runge-Kutta method was applied to numerically integrate the equations with the time width equivalent to 11.025 [kHz]. After discarding the initial transient part of x_1, x_2 and x_3, the speech signal was added to x_2 as dynamical noise in the drive system. Then, the x_2 signal containing the speech signal was transmitted to the response system. The maximum amplitude of the speech signal relative to that of the carrying signal was adjusted to be $\| m \| / \| x_2 \| \approx 10^{-4}$.

Figure 1 displays the original speech signal "Yes, we can". The chaotic signal x_2 containing the time-integrated message generated by the drive system and the chaotic signal y_2 retrieved using the OPCL control method by the response system are shown in Figs. 2 and 3, respectively. There was no discernible difference in between x_2 containing the message and y_2. That is, the encrypted signal sounded like noise containing no audible message. The message decrypted by the response system is shown in Fig. 4. For comparison, we show the same part of the speech signal before and after encryption and decryption in Figs. 5 and 6, respectively. The decrypted message is substantially similar to the original message shown in Fig. 1, although it sounded slightly noisy comparing with the original message. These observations indicate that our method for secure communications works as expected.

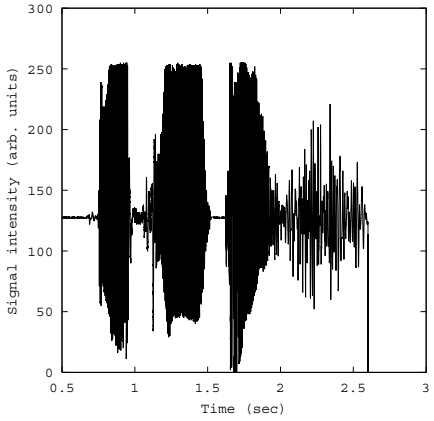

Figure 1: Original message "Yes, we can."

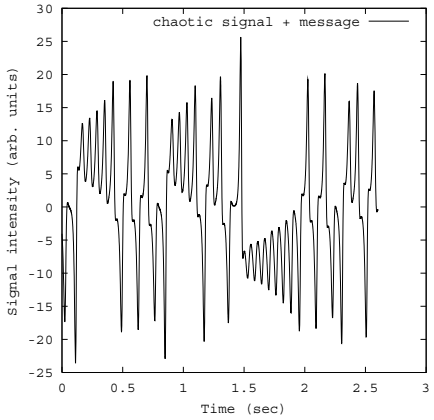

Figure 2: Chaotic signal x_2 containing message generated by drive system.

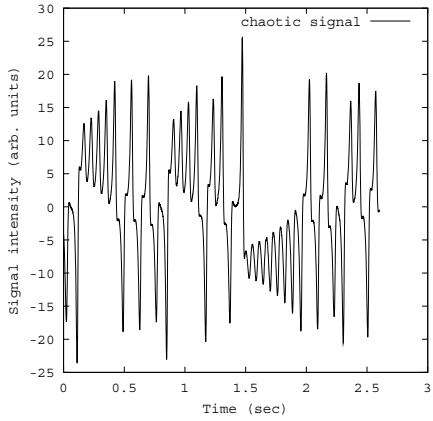

Figure 3: Chaotic signal y_2 retrieved by response system.

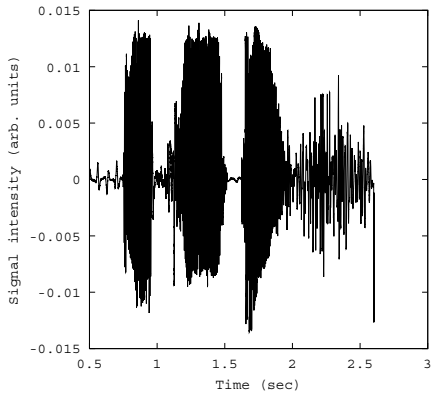

Figure 4: Decrypted message.

4. Discussion

In our method, the message is treated as dynamical noise added to a state variable of the chaotic oscillator of the drive system when encrypting a message. The variable should be selected in terms of the exclusiveness of a parameter mismatch in multiplying it with the variable. Thus, the message is viewed as part of the parameter mismatch. This is in contrast to Cuomo-Oppenheim's method in which a message is superimposed as additive (observational) noise on a carrying signal when transmitted to the response system. The message is decrypted using chaotic synchronization by OPCL coupling between the chaotic oscillators in drive and response systems having parameter mismatch. The parameter mismatch is an indispensable key for decryption. The response system cannot retrieve the message from the received signal without knowledge of the parameter mismatch. When the chaotic oscillators have multiple parameters and parameter mismatches, we can achieve multiplex encryption and decryption of multiple messages. This has recently been shown using chaotic oscillators subject to the Lorenz equations by the authors [8].

Another benefit of our method is also brought about by the use of OPCL coupling. It makes our method free of the negativity of the conditional Lyapunov exponents indispensable for the stability of the synchronization manifold. In fact, we have not considered the conditional Lyapunov exponents in the present experiment using the Sprott oscillators. This allows us a wide selection of the dynamics governing the chaotic oscillators installed on drive and response systems.

5. Conclusion

We have shown the applicability of the OPCL control method to chaos-based communications through our experiment for the encryption and decryption of the speech signal. Our method provides two benefits that

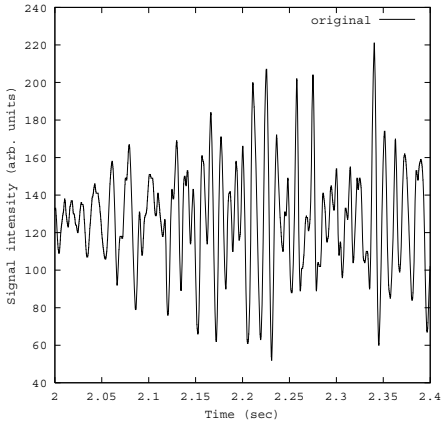

Figure 5: Part of original message (before encryption).

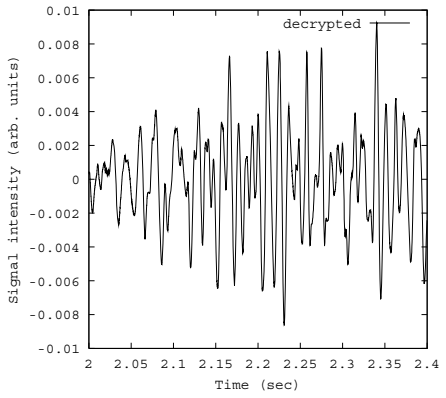

Figure 6: Part of decrypted message.

are absent in Cuomo-Oppenheim-Strogatz's method. One is freedom from negativity of the conditional Lyapunov exponents in selecting the dynamics governing the chaotic oscillators. The other is the use of parameter mismatch between the oscillators as the key for encryption and decryption. However, our recent work has revealed a weak point of our method that a message cannot be entirely masked by a carrying signal in the frequency domain [8], which remains to be studied as an open problem.

Acknowledgment

We appreciate Mr. Shuji Nakamura and Mr. Tatsuya Kunioka for their technical support.

References

[1] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems," Phys. Rev. Lett., vol.64, no.8, pp.821–824, 1990.

[2] H. Nijmeijer and I. M. Y. Mareels, "An Observer Looks at Synchronization," IEEE Trans. Circuits Syst. I, vol.44, no.10, pp.882–890, 1997.

[3] K. M. Cuomo and A. V. Oppenheim, "Circuit Implementation of Synchronized Chaos with Applications to Communications," Phys. Rev. Lett., vol.71, no.1, pp.65–68, 1993.

[4] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," IEEE Trans. Circuits Syst. II, vol.40, pp.626–633, 1993.

[5] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fisher, J. Garcia-Ojarvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature, vol.437, pp.343–346, 2005.

[6] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic Cryptosystems: Cryptanalysis and Identifiability," IEEE Trans. Circuits Syst. I, vol.53, no.12, pp.2673–2680, 2006.

[7] D. Arroyo, S. Li, C. Li, and V. Fernandez, "Cryptanalysis of a New Chaotic Cryptosystem Based on Ergodicity," Int. J. Mod. Phys. B, vol.23, pp.651–659, 2009.

[8] T. Miyano, K. Nishimura, and Y. Yoshida, "Chaos-Based Communications Using Open-Plus-Closed-Loop Control," unpublished.

[9] I. Grosu, R. Banerjee, P. K. Roy, and S. K.Dana, "Design of coupling for synchronization of chaotic oscillators," Phys. Rev. E, vol.80, pp.016212-1–016212-8, 2009.

[10] I. Grosu, E. Padmanaban, P. K. Roy, and S. K. Dana, "Designing Coupling for Synchronization and Amplification of Chaos," Phys. Rev. Lett., vol.100, pp.234102-1–234102-4, 2008.

[11] I. Grosu, "General Coupling for Mutual Synchronization of Three Identical Oscillators," Int. J. Bifurcation Chaos Appl. Sci. Eng., vol.17, no.10, pp.3519–3522, 2007.

[12] I. Grosu, "Robust synchronization," Phys. Rev. E, vol.56, no.3, pp.3709–3712, 1997.

[13] E. A. Jackson and I. Grosu, "An open-plus-closed-loop (OPCL) control of complex dynamic systems," Physica D, vol.85, pp.1–9, 1995.

[14] J. C. Sprott, "Some simple chaotic flows," Phys. Rev. E, vol.50, no.2, pp.R647–R650, 1994.