Chaotic Communication via Temporal Transfer Entropy

Yao-Chen Hung[1] and Chin-Kun Hu[1,2,*]

[1]*Institute of Physics, Academia Sinica, Nankang, Taipei 11529, Taiwan*

[2]*Center for Nonlinear and Complex Systems and Department of Physics, Chung Yuan Christian University, Chungli 32023, Taiwan*

(Received 22 July 2008; published 12 December 2008)

We propose a new perspective on communication using chaos. A binary message is encoded into the temporally causal relations on a coupled maps ring of N chaotic nodes. From the analysis of temporal transfer entropy, the masked information can be recovered from transmitted signals at the receiver. The communication scheme has been demonstrated to be robust against external noise and some traditional attacks.

DOI: 10.1103/PhysRevLett.101.244102 PACS numbers: 05.45.Vx, 05.45.Tp, 89.70.−a

The detection of causality, also known as the drive-response relationship, between measured signals has attracted much attention in recent years [1–3]. The causality assessment is to evaluate the variance of predictability of one series by incorporating information of the other. If the predictability is consequently enhanced, then the latter is identified as a driver which has a causal influence on the former. Several methods have been proposed and successfully applied to artificial models and recorded data with the assumption of stationarity [1,2]. Applications of them arise in many different fields, such as physics, physiology, neurophysiology, economy, and climatology [3].

In this Letter, we apply the concept of causality and its measurement to a different field: the chaotic communication. The basic idea for chaotic communication is to make use of the chaotic nature of the carrier to encrypt a sequence of messages. Two typical techniques include the chaotic masking approach and the chaotic modulation method [4]. Several variants and refinements of the two methods had been proposed, for instant the use of different levels of synchronization, different portraits of chaotic carriers, different techniques of chaos control, and different expressions of communication schemes [5]. The common point of these methods is the reliance on synchronization [6,7]. Here we develop a counterintuitive scheme which hides binary messages in causal relationships on a couple-map ring (CMR) consisting of chaotic elements. That is, the clockwise or counterclockwise coupling on the ring indicates the bipolar data $\mu^k = 1$ or $\mu^k = 0$. The time series of two adjacent maps are used as transmitting signals through public channels. At the receiver, encrypted messages are recovered by a proposed measure, the temporal transfer entropy (TTE), based on information theory. It has been demonstrated that the scheme is robust against external noise and some traditional attacks. The technique also provides us a new perspective toward chaotic communication.

Communication scheme.—The core idea of this Letter is to utilize the temporal causality of coupled chaotic systems for messages encryption and transmission. We have chosen an one-dimensional unidirectionally CMR of N nodes as the chaotic generator to encrypt transmitted messages, as showed in Fig. 1(a). The dynamics of the subsystem S_n at the nth node of the CMR is given by

$$x_n(t+1) = f((1-\varepsilon)x_n(t) + \varepsilon X_n(t)), \qquad (1)$$

where $n = 1, 2, \ldots, N$, t is the time index, $X_n(t)$ is the driving force from the nearest systems $S_{n\pm1}$, and coupling strength $\varepsilon = 0.5$ is chosen throughout the Letter. We choose the Ulam map $f(x) = 2 - x^2$ as the local chaotic dynamics. One can also choose other chaotic maps.

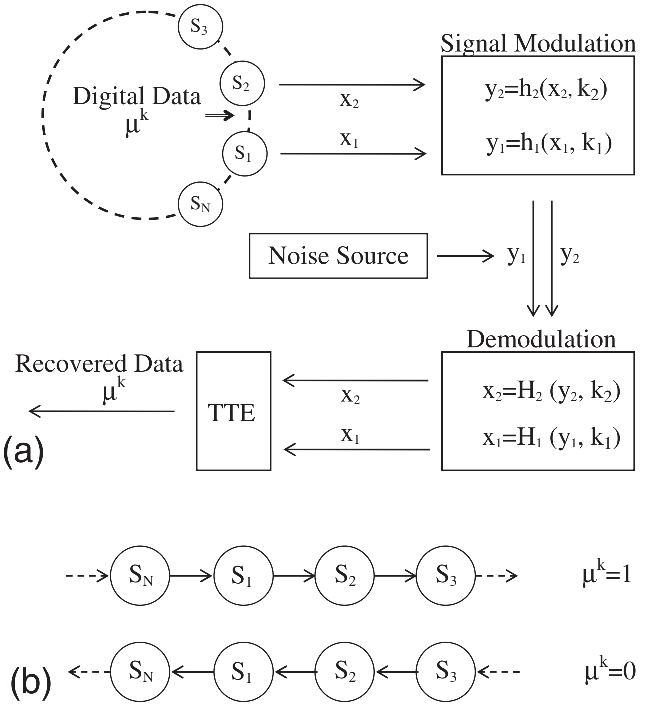

FIG. 1. (a) Communication scheme based on temporal causality of the coupled maps ring. (b) Encoding process of the binary information.

To encode a series of K binary information μ^k ($k = 1, \ldots, K$) into the instantaneous causal relations of the CMR, we choose the following driving term:

$$X_n(t) = \begin{cases} x_{n-1}(t) & \text{if } \mu^k = 1, \\ x_{n+1}(t) & \text{if } \mu^k = 0, \end{cases} \tag{2}$$

as drawn in Fig. 1(b). The reason why we use the CMR is to keep the phase portraits of subsystems invariant under every reversion of the coupling direction. The invariability then prohibits intruders from mining the message by the technique of return maps [8].

The outputs of the CMR containing message information are communicated to the receiver over public channels. Here we select the iterations of $x_1(t)$ and $x_2(t)$ as the carriers. For security, $x_1(t)$ and $x_2(t)$ are further modulated by specific functions $h_1(x_1(t), k_1)$ and $h_2(x_2(t), k_2)$; here $k_{1,2}$ are security keys, which are preknown by the receiver. Modified signals $y_1(t)$ and $y_2(t)$ are then transmitted to the receiver and demodulated by inverse functions $H_{1,2} = h_{1,2}^{-1}$. Finally, the cipher messages can be retrieved by monitoring the temporal causality between the series $x_1(t)$ and $x_2(t)$.

Temporal transfer entropy.—Among present methods of assessing causality, transfer entropy (TE) [1] is the most reliable one because of its solid mathematical foundation of information theory. We start with the method and further generalize it in this Letter to detect the temporal variation of coupling directions. Here we briefly review the basics of information theory and the concept of TE. For a physical process I with probabilities $\{p(i)\}$ visiting the states $\{i\}$, Shannon entropy can be defined by $H(I) = -\sum_i p(i) \log_2 p(i)$. Such a measur provides a convenient way to calculate the average minimum number of bits needed to encode the physical process. The base number 2 only defines the unit as bit and will be neglected hereafter.

If we introduce another process J with probability distribution $\{p(j)\}$ and joint probability $\{p(i, j)\}$, the average information gained about I by the knowledge of J is given by

$$M_{IJ} = \sum_{i,j} p(i, j) \log \frac{p(i, j)}{p(i)p(j)}, \tag{3}$$

which is the well-known mutual information (MI). MI is reliable to discover nonlinear dependencies (or couplings) between systems of interest. Unfortunately, as a result of the symmetric property, it does not contain any directional information and becomes invalid in the causality analysis. To overcome this fault, recently a modified measure was proposed by incorporating the ideas of Markov property and Kullback entropy. Denoting the state of the process I at time τ as i_τ and time $\tau + 1$ as $i_{\tau+1}$, Schreiber [1] defined the measure to detect asymmetry dependence of I on J by

$$\mathrm{TE}_{J,I} = \sum p(i_{\tau+1}, i_\tau, j_\tau) \log \frac{p(i_{\tau+1}|i_\tau, j_\tau)}{p(i_{\tau+1}|i_\tau)}. \tag{4}$$

For practical applications, the joint probability and conditional probability distributions can be evaluated from time series by simple box-counting algorithm or kernel estimation. TE then provides us an excellent estimation to identify the causal relations of systems of interest.

In general cases, the causality does not keep invariant with time passing. For instance, in the years 2001 and 2002 trading activities in the Dow Jones Industry Average (DJIA) influenced NASDAQ more than NASDAQ influenced the DJIA, while the causal relation was reversed in years 1998, 1999, and 2003 [9]. Similar examples appear in neuroscience, climate, biological networks, etc. In our communication scheme, the encrypted symbols defining the coupling directions of CMR vary ceaselessly to encode messages. The measure defined by Eq. (4) cannot detect the nonstationary causal relations.

To take the nonstationary effect into consideration, we modified the TE by adopting a different algorithm, the skewed probability distribution, which has already been introduced with the concept of causal entropy (CE) [10]. The probability distribution is updated once a new event is generated. In other words, the distribution $\{\hat{p}(l)\}_t$ evolves with time. If the latest event visited the states l_e, the appropriate probability is increased by a fixed value Δp. Otherwise, the others are fixed invariably. After every update, the appropriate distribution is renormalized. Thus,

$$\hat{p}(l)_{t+1} = \begin{cases} \frac{\hat{p}(l)_t + \Delta p}{1+\Delta p} & \text{if } l = l_e, \\ \frac{\hat{p}(l)_t}{1+\Delta p} & \text{otherwise.} \end{cases} \tag{5}$$

The central core of such an algorithm is to enhance the weight of probability of the latest event. Thus, the probability distribution is skewed toward the new events. Applying it to calculate the time-dependent distribution of joint and conditional probabilities, we can get

$$\mathrm{TE}^t_{J,I} = \sum \hat{p}(i_{\tau+1}, i_\tau, j_\tau)_t \log \frac{\hat{p}(i_{\tau+1}|i_\tau, j_\tau)_t}{\hat{p}(i_{\tau+1}|i_\tau)_t}, \tag{6}$$

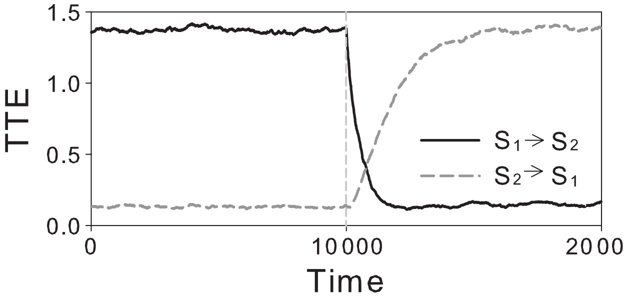

FIG. 2. Temporal transfer entropies $\mathrm{TE}^t_{S_1,S_2}$ and $\mathrm{TE}^t_{S_1,S_1}$ as functions of time for a CMR of Ulam maps. At $t = 10^4$, the coupling direction is reversed. The two qualities of TTE clearly reflect the variation of the causality.

where the sum runs over all states. Equation (6) now allows dynamically monitoring the change of causality between coupled systems. We call the modified measure the temporal transfer entropy (TTE).

The aforementioned CMR with the size $N = 100$ is taken as our test model to examine the reliability of the measure. For the duration of long transients ($\sim 10^5$) and $t < 10^4$, the coupling direction is from the map S_n to the map S_{n+1}, while the coupling is reversed after $t > 10^4$. By discarding the transients, $\Delta p = 10^{-3}$ is used to compute the entropies $\mathrm{TE}^t_{S_1,S_2}$ and $\mathrm{TE}^t_{S_2,S_1}$. The joint probability distributions of systems S_1 and S_2 are computed using simple box counting with eight equidistant bins and the initial distributions $\{\hat{p}(l)\}_{t=0}$ of S_1 and S_2 are collected from the transients. The numerical results are shown in Fig. 2. For the duration of $t < 10^4$, we clearly notice the significant predominance of $\mathrm{TE}^t_{S_1,S_2}$ over $\mathrm{TE}^t_{S_2,S_1}$, which indicates the coupling directing from S_1 to S_2. After $t > 10^4$, values of $\mathrm{TE}^t_{S_1,S_2}$ and $\mathrm{TE}^t_{S_2,S_1}$ reflect the reversion of causality of two systems; i.e., $\mathrm{TE}^t_{S_2,S_1}$ predominates over $\mathrm{TE}^t_{S_1,S_2}$.

Note that after tuning the causality, it takes some transitions for both qualities to evolve from the presaturated state to the postsaturated state. The time interval required for the transition process is called the relaxation time labeled as T_R. Actually, the qualities of T_R strongly depend on the choice of Δp. As illustrated in Fig. 3(a), the functional relation of Δp and T_R obeys a specific power law. As one can observe, the relaxation time of the transition from a predominant state to an inferior state (circles) is shorter than the one required for the reverse transition (triangles) with respect to an identical Δp, although both transitions share an identical exponent ~ -1.1 in the log-log plot. Moreover, with the increase of Δp the distinction between the predominant state and the inferior state withers accordingly. The dependence of TTE on the quantities of Δp is shown in Fig. 3(b), where the error bars embrace 2 standard deviations of the distribution of TTE over long evolutions.

Since TTE is able to monitor the direction of causality, the next step is the evaluation of the scheme to encrypt and decrypt a message. We introduce a series of binary messages μ^k with the length of each information bit T_μ, shown in Fig. 4(a). To enhance communication efficiency, we choose $T_\mu = 200$. A specific sequence is taken for the promoter which labels out the initiation of the meaningful message ($t = 0$ in the figure). As mentioned above, μ^k is modulated into the causal relations in the CMR, and signals $x_1(t)$ and $x_2(t)$ are served as chaotic carriers. The modulation function is chosen as $h(x) = x$ to simplify the analysis. At the receiver, the encrypted data is decoded by the analysis of TTE, and Δp is chosen as 0.02 to accelerate the relaxation process. We plot values of TTE as a function of time in the directions of $S_1 \rightarrow S_2$ (blue solid line) and $S_2 \rightarrow S_1$ (red dotted line) in Fig. 4(b). To facilitate the decryption, a quality σ^k is defined to evaluate the predominance of coupling directions,

$$\sigma^k = \sum_{kT_\mu + t'}^{(k+1)T_\mu} (\mathrm{TE}^t_{S_1,S_2} - \mathrm{TE}^t_{S_2,S_1}), \tag{7}$$

where $t' = 50$ is chosen to reduce the effect of relaxation. The quality σ^k is positive if the information bit $\mu^k = 1$, otherwise negative. The encrypted messages then can be successfully recovered by the sign of σ^k, as presented in Fig. 4(c).

Robustness.—We further consider the performance of the method with respect to robustness and security. To evaluate the robustness of the proposed scheme against the influence of external noise, we calculate the probability of recovering a bit incorrectly under various noise levels. We added two independent sequences of Gaussian noise to the carriers $x_1(t)$ and $x_2(t)$, respectively, and compared the

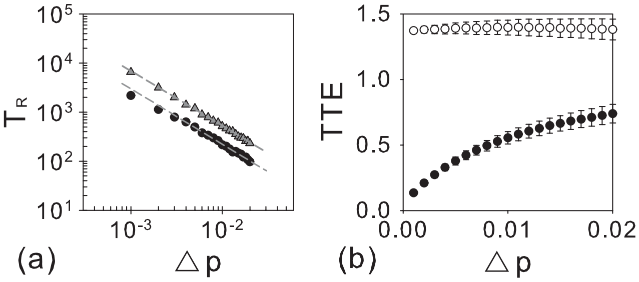

FIG. 3. (a) Relaxation times T_R as functions of Δp. The slope of the reference lines is -1.1. (b) The dependence of TTE on Δp. With the increase of Δp, the distinction between the predominant state (empty circles) and the inferior state (solid circles) becomes smaller.

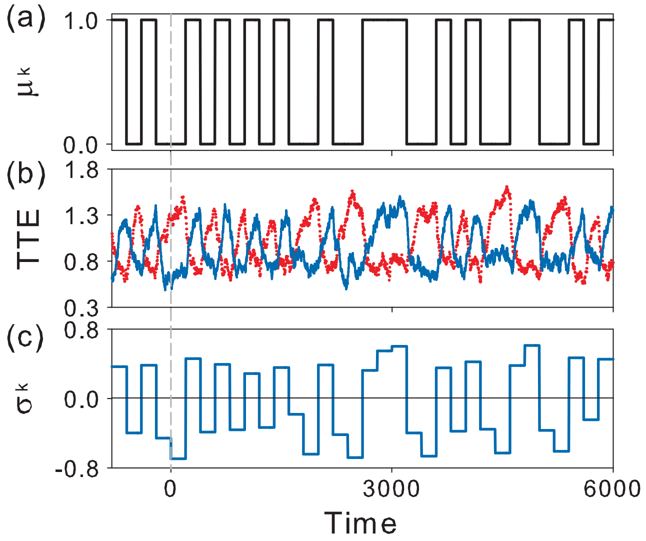

FIG. 4 (color). (a) A sequence of binary messages μ^k with the length of each information bit $T_\mu = 200$. (b) The evolution of TTE in the directions of $S_1 \rightarrow S_2$ (blue solid line) and $S_2 \rightarrow S_1$ (red dotted line). (c) The sequence of σ^k: $\sigma^k > 0$ indicates $\mu^k = 1$, while $\sigma^k < 0$ indicates $\mu^k = 0$.

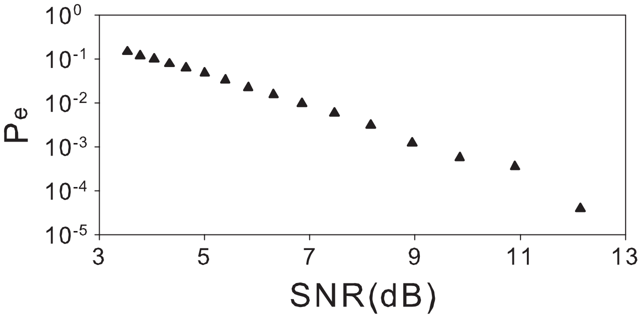

FIG. 5. The error probability P_e versus the signal-to-noise-ratio (SNR). In each simulation, 10^5 randomly generated symbols are transmitted.

decoded binary message to the original one. Figure 5 shows the error probability P_e as a function of the signal-to-noise-ratio, SNR(dB) [11]. The result shows that the scheme has a high noise tolerance capability and thus, the system is feasible.

When crypt-analyzing a communication scheme, the general assumption is that intruders know exactly the decoding mechanism at the receiver. In other words, they are familiar with the technique of TTE and have the modulation functions $h_1(x_1, k_1)$ and $h_2(x_2, k_2)$ except the security keys k_1 and k_2. Here we adopt an algorithm for $h_1(x_1, k_1)$ and $h_2(x_2, k_2)$ to consider the security issue. In real applications of detecting causality, it is important to access the significance of the measured value of TE. To this end, the original data are shuffled in time and consequently all potential correlations between two processes I and J are destroyed [3]. A significant threshold confirming the information direction is then determined by calculating TE with the shuffled data. Based on the concept of the surrogate data, a candidate for the modulation function is the Knuth shuffle algorithm [12] which shuffles $x(t)$ through a random number generator using a specific seed. The seed therefore is used as the security key k to recover the modulated signal through a reverse function, $x(t) = H(y(t), k)$. Owing to the high obscurity of causality assessment, it is hard for attackers to reduce the key space even though they can get some original messages and their corresponding cipher messages. Other modulation functions which eliminate the causal relations between chaotic carriers are available.

By incorporating the concept of synchronization, the communication scheme can be refined further. For example, suppose S_n^A and S_n^B are the n-th nodes on two CMRs which share identical formulae but evolve from different initial conditions. The couplings are directed from S_n^A or S_n^B to a single node S_0 if the symbols 1 or 0 are encoded. The iterations of S_0 are transmitted to the receiver over a public channel. At the receiver, one replica of CMRs is presynchronized with one of the originals and TTE is applied to detect the causality between S_0 and the replica of S_n^A (or S_n^B). In this scheme, the parameter sets of CMRs are served as the security keys.

In brief, we have demonstrated that the processes of encoding and decoding temporal causality can be used in chaotic communications. The availability of TTE in continuous-time and multidimensional problems has also been confirmed [13]. The proposed scheme is promising for the encryption of messages and deserved further investigations in various directions, such as the enhancement of efficiency, realization by means of electronic circuit or multimode solid-state laser [3], etc. The proposed nonlinear measurement, TTE, can be further applied to monitor causal relationships between dynamical systems.

This work was supported by Grant NSC 96-2911-M 001-003-MY3 and NCTS (North) in Taiwan. We thank Gang Hu, Zbigniew Struzik, and Ming-Chya Wu for helpful discussions.

*huck@phys.sinica.edu.tw

[1] T. Schreiber, Phys. Rev. Lett. **85**, 461 (2000).

[2] R. Q. Quiroga, J. Arnhold, and P. Grassberger, Phys. Rev. E **61**, 5142 (2000); M. Paluš *et al.*, *ibid.* **63**, 046211 (2001); X. Hu and V. Nenov, *ibid.* **69**, 026206 (2004).

[3] P.F. Verdes, Phys. Rev. E **72**, 026222 (2005); R.Q. Quiroga *et al. ibid.* **65**, 041903 (2002); K. Otsuka *et al. ibid.* **69**, 046201 (2004).

[4] K.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[5] A. Wagemakers, J.M. Buldú, and M.A.F. Sanjuán, Europhys. Lett. **81**, 40 005 (2008); X.-J. Wu, Chaos **16**, 043118 (2006); J.Y. Chen *et al.*, Chaos **13**, 508 (2003); and references therein.

[6] L.M. Pecora and T.L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

[7] A.S. Pikovsky, M.G. Rosenblum, and J. Kurths, *Synchronization: A Universal Concept in Nonlinear Sciences* (Cambridge University Press, Cambridge, England, 2004); P.M. Gade and C.-K. Hu, Phys. Rev. E **60**, 4966 (1999); **62**, 6409 (2000); **73**, 036212 (2006); Y.-C. Hung *et al.*, *ibid.* **77**, 016202 (2008).

[8] A.A. Minai and T.D. Pandian, Chaos **8**, 621 (1998).

[9] M.C. Wu *et al.*, Phys. Rev. E **73**, 016118 (2006).

[10] R. Dzakpasu *et al.*, Chaos **16**, 043121 (2006).

[11] K. Murali, Phys. Rev. E **63**, 016217 (2000).

[12] D.E. Kunth, *The Art of Computer Programming* (Addison Wesley, Reading, Massachusetts, 1998), 3rd ed., p. 145.

[13] Y.C. Hung, Y.-T. Huang, and C.-K. Hu (unpublished).