gustav / January 04, 2009 05:59PM
[應用物理]中研院物理所研究團隊獨創混沌通訊加密方法
中研院物理所研究團隊獨創混沌通訊加密方法

中研院物理研究所「統計與計算物理實驗室」研究員胡進錕教授與物理研究所博士後研究員洪耀正，日前提出一個嶄新的「瞬間轉換熵」（Temporal Transfer Entropy）觀念，為傳統通訊傳遞方式頻遭破解的窘境，找到嶄新加密方法。這篇論文已於2008年12月12日發表於《物理評論通訊》(Physical Review Letters)，由於此概念應用層面相當廣泛，可望受到國際學術界和產學界的高度重視。

傳統的混沌加密方式，是將想要隱藏的資訊，加載於由混沌信號所構築的載波裡。藉由載波紊亂、無序的特性，使第三者無從獲悉加密者所欲傳遞的訊息。然而隨著訊號析離技術的發展，這樣的方式已經不敷使用。

利用混沌載波間的因果相關性（Causality）來編撰二元訊息，訊息不再包含於混沌載波之中，而是載波與載波間具有方向性的瞬時相關性。在轉譯出訊息時，以訊息理論（Information Theory）為基礎，引入了「瞬間轉換熵」（Temporal Transfer Entropy）的概念，以監控並量取因果相關性的瞬時變化。如此一來，知情者眼中意涵豐富的二元符號便在外人眼中看似沓亂隱晦的數字陣列。

這項「瞬間轉換熵」的分析工具，還可進一步應用到其它不同領域，諸如醫學、經濟學、以及氣象學等學科。例如，癲癇症患者在進行外科手術切除大腦局部前，必須明確地定位出癲癇發作區間以減少手術對病人腦部的傷害。藉由腦波訊號的紀錄以及即時因果相關性的分析，醫師將可準確掌握發作部位從而降低手術造成的損傷。而藉由此工具分析歷年來溫度變化、二氧化碳濃度變化等數據資料，也有助於釐清造成地球暖化現象的因果關係。

An Innovative Encryption Method in Chaotic Communication Presented by LSCP, Academia Sinica

The researcher Professor Chin-Kun Hu and the postdoctoral researcher Yao-Chen Hung of the Laboratory of Statistical and Computational Physics, Institute of Physics, Academia Sinica Taiwan, proposed a new idea "temporal transfer entropy (TTE)," finding a new encryption method to improve the weak defense of the traditional method. The article about this idea was presented in 《Physical Review Letters》 12th-Dec, 2008. The conception enjoys a wide range of application; it is meant to draw much academic as well as industrial attention in the world.

Traditional chaotic encryption method is to make use of the chaotic nature of the carriers to encrypt the target information so that the third side can not understand it. However, along with the development of signal separation skills, the method and its refinement get insufficient.

Hiding binary messages in causal relationships on a couplemap ring consisting of chaotic elements, signals are no longer contained in the carriers; they are contained in the instantaneous directional correlations between carriers. At the receiver, encrypted messages are retrieved with the proposed measure "temporal transfer entropy" (based on information theory), so that the change of causality between coupled systems gets under monitoring.

The measure "temporal transfer entropy" can find its application in other fields as well such as medicine, economics, meteorology etc. For instance, before the brain operation on an epileptic, it is significant to be able to identify the location of the breakout area. With the analysis result about the recording of brain waves and its causal relations, the surgeon can precisely locate the breakout area and decrease the damage probability. The measure can also help with analyzing data such as the change of global temperature or the change of the thickness of carbon dioxide.

深入資訊Further Information：
統計與計算物理實驗室 http://www.sinica.edu.tw/~statphys/

聯繫資訊Contact Information：
胡進錕博士Dr. Hu，中央研究院物理研究所研究員ASIP Research Fellow，(Tel)886-2-2789-6720
林美惠Ms. Lin，中央研究院總辦事處公關室AS-PR Office
(Tel)886-2-2789-8821、(Fax)886-2-2782-1551、(M)0921-845-234

Edited 3 time(s). Last edit at 01/11/2009 10:48AM by gustav.