IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 3, Mar 2014, 163-172

SCCE: SECURE COMMUNICATION BASED ON A CHAOTIC SYSTEM FOR MODERN WIRELESS COMMUNICATION

P. KARTHIK[1], P. S. RANJITH[2] & M. JAYAGANESH[3]

[1]Assistant Professor, Department of Electronics and Communication Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India

[2,3]Under Graduate Scholar, Department of Electronics and Communication Engineering, Anna University, SNS College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

Wireless communication networks use interconnected devices within a relatively small area that is generally within a person's reach. The term Wireless network is defined as a network, which is of any type and uses some form of wireless network connection and hence more susceptible to malevolent attacks. The present system is encrypted based on algorithms and certain proposed standards which detects and restricts the high malevolent behaviour detection rates in certain circumstances, which does not greatly affect the network performances by using a digital signature algorithm, S-ACK (secure acknowledgment). However the wide usage of algorithms and proposed standards are published and the methodologies are exposed to the world's view. In an instance it allows the hackers to intrude any type of communication systems and made them vulnerable to attacks. Hence, by adopting the different methodologies rather than the existing methodologies enhances the security. The suggested system is to overcome the drawbacks of existing encryption methodologies such as DES, RSA by enhancing the security of the data by the chaotic encryption method. This method involves the use of commutative codes and above algorithms to reassure the security of the transmitted data. By adopting the above technique the data transmission and reception is highly secure than existing methods.

KEYWORDS: Wireless Communication Networks, Digital Signature Algorithm, Malevolent Behaviour, DES, RSA, Chaotic Encryption Method

INTRODUCTION

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can communication process. It is a discipline of defending information by coding it into an indecipherable layout. Cryptography is an active technique of defending delicate data as it is stored on media or transmitted over linkage communication pathways. Even though the definitive goalmouth of cryptography, and the mechanism that evolves it up, is to safeguard information from unlicensed persons, most algorithms can be hacked and the data can be revealed if the intruder has enough time, desire, and resources. So a more genuine goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker.

Encryption methods evolved from being mainly for show into practical applications used to hide information from others. As encryption evolved, it was mainly used to pass messages through hostile situations of war, issues, and for intervention processes between conflicting groups of people. Throughout antiquity, entities and regimes have

worked to protect communication by encrypting it. As time gets passed, the encryption algorithms and the devices that used them to increase in complexity, new procedures and regulations were continually introduced, and it became a unified part of the computing world. Encryption means that message signal is being converted into streams of binary code that passes over network cables, internet communication ways, and air as a medium for waves. Today, the transmission mechanism has changed from human beings to packets carrying 0's and 1's passing through network cables or open airwaves. The data are still encrypted in situation an intruder captures the transmission mechanism (the packets) as they travel along their paths. This simplistic encryption method worked for its time and for particular cultures, but eventually more complex mechanisms were required. As computers came to be, the possibilities for encryption methods and devices, modernized, and cryptography efforts expanded drastically. This era brought extraordinary opportunity for cryptographic designers and encryption techniques. The most well-known and thriving project was Lucifer, that was developed at IBM. Lucifer introduced complex mathematical equations and functions. Intrusion detection is that the method of observing the events occurring in a very ADP system or network and analyzing them for signs of intrusions, outlined as makes an attempt to compromise the confidentiality, integrity, handiness, or to bypass the protection mechanisms of a PC or network.

IMPLEMENTATION TOOL

MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language. Developed by Math Works, Developed by Math Works, Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and knowledge, implementation of algorithms, creation of user edges, and interfacing with programs written in alternative languages, together with C, C++, Java, and Fortran. Java, and FORTRAN. MATLAB is a simulation tool that is helpful in finding out the dynamic nature of the communication networks. The Communication System Toolbox provides algorithms for manipulating, simulating, and examining communications systems. These competences are unit provided as MATLAB functions, MATLAB System object, and Simulink blocks. The system toolbox enables source cryptography, channel cryptography, interleaving, modulation, deed, synchronization, and channel modelling. The Communication System Toolbox in MATLAB also provides functions and scripts to detect the presence of intrusion and Denial of Service attack in the communication network which helps to improve the security of the communication channel.

RECENT ENCRYPTION TECHNIQUES

The three simple methods of cryptography in common use symmetric key, asymmetric (public) key systems and cryptographic hash functions. The three basic systems involve with the usage of standardized algorithms.

Ciphers

A Hebrew cryptographic method required the alphabet to be flipped so that each letter in the original alphabet is mapped to a different letter in the flipped alphabet. The encryption method was called abash. For example, the word "security" is encrypted into "hvxfirgb." In a transposition cipher, permutation is used, meaning that the letters are twisted. The key is limiting the points that the characters are moving.

Cipher Machine

The rotor cipher machine, which is a device that substitutes letters using different rotors within the machine, was a

huge innovation in martial cryptography that provided complexity that proved difficult to break. The originator of the message configured the Enigma machine to its initial settings before starting the encryption method. The handler would type in the first letter of the message and the machine would substitute the letter with a different letter and present it to the operator. This encryption was completed by changing the position of the rotors a predefined number of times, which would substitute the original letter with a different letter. Hence, when the typewriter, typed the T as a first letter as a first character, the enigma machine should present S as a substitution character. The operator should write down the letter M on the sheet. Then the operator should advance the rotor for further operation. Each time a new letter was to be encrypted, the operator must advance the rotor to a new setting. This process was done until the whole message was encrypted.

Algorithm

An algorithm is an effective method expressed as a finite list of well-defined instructions for manipulating a function. Starting from an early stage and preliminary input the instructions describe an evaluation that, when accomplished, continues through a finite number of well-defined successive states, eventually producing "output" and terminating at a final finish state. The changeover from one formal to the next is not necessarily deterministic; some algorithms, known as probability based algorithms, integrate random input. Intrusion detection is that the method of observing the events occurring in a very ADP system or network and analyzing them for signs of intrusions, outlined as makes an attempt to compromise the confidentiality, integrity, handiness, or to bypass the protection mechanism.

SYNCHRONIZATION OF CHAOS

Synchronization of chaos could be a development which will occur once two, or more, dissipative chaotic systems are coupled. As a result of the exponential divergence of the close trajectories of chaotic systems, having two chaotic systems evolving in synchronization would possibly seem shocking [1]. However, synchronization of coupled or driven chaotic oscillators could be a development well established through an experiment and fairly well understood in theory. Synchronization of chaos could be a wealthy development and a multi-disciplinary discipline with broad variance applications. The synchronization might gift a range of firms looking at the character of the interacting systems and of the coupling theme.

IDENTICAL SYNCHRONIZATION

This type of synchronization is also known as complete synchronization. It can be observed in identical chaotic systems. The systems are said to be totally synchronized when there is a set of preliminary conditions so that the systems ultimately evolve similarly in time [2]. In the case of two diffusively coupled dynamics are described by

$$x' = F(x) + \alpha(y-x)$$

$$y' = F(y) + \alpha(x-y)$$

Where F is the vector field modelling the isolated chaotic dynamics and α is the coupling parameter. The regime x (t) =y (t) defines an invariant subspace of the coupled system, if this subspace x (t) =y (t) is locally attractive then the coupled system exhibit identical synchronization [8].

If the coupling vanishes the oscillators are detached, and the chaotic response leads to a deviation of nearby paths[3]. Complete synchronization occurs due to the interaction, if the coupling factor is large enough so that the

disagreement of paths of interacting systems due to chaos is suppressed by the diffusive coupling. To find the acute coupling strength we study the behaviour of the difference v = x-y Assuming that ϒ is small we can expand the vector field in the series and obtain a linear differential equation - by neglecting the Taylor remainder - governing the behaviour of the difference[2]

$$v' = DF(x(t))\, v - 2\alpha v$$

Where DF (x (t)) denotes the Jacobian of the vector field along with the solution. If $\alpha = 0$ then we obtain

$$u' = DF(x(t))u,$$

and since the dynamics of chaotic we have $\| u(t) \| \leq \| u(0) \| e^{\lambda t}$, where λ denotes the maximum Lyapunov exponent of the isolated system. Now using the Ansatz $v=ue^{-2\alpha t}$ we pass from the equation for ν to the equation for. Therefore, we obtain

$$\|V(t))\| \leq \|u(0)\| e^{(-2\alpha+\lambda)t}$$

yield a critical coupling strength $\alpha_c = \lambda/2$, for all $\alpha \geq \lambda$ the system exhibit complete synchronization. The presence of a critical coupling efficiency is associated with the chaotic nature of the isolated dynamics[4]. In general, this reasoning leads to the correct critical coupling value for synchronization. Likely, in a few cases, one might observe loss of synchronization for coupling level, higher than the acute value. This happens because the nonlinear terms neglected in the source of the threshold coupling value can play an important role and destroy the exponential bound for the behaviour of the difference[6]. It is, however, possible to give a rigorous treatment to this problem and obtain a critical value so that the nonlinearities will not affect the stability.

CHAOS AND HYPERCHAOS

Hyperchaos Synchronization Using PSO-Optimized RBF-Based Controllers

This method uses a standard RBF neural controller. Particle swarm optimization (PSO) algorithm is used to derive and optimize the parameters of the RBF controller. In the second method, with the aim of increasing the robustness of the RBF controller, an error integral term is added to the equations of RBF neural network. For this method, the coefficients of the error integral component and the parameters of RBF neural network are also derived and optimized via PSO algorithm[5]. For better comparison, the proposed methods and an optimal PID controller optimized by PSO are applied to the Lorenz hyperchaotic system for secure communication. The simulation results show the efficiency and the dominance of the proposed methods in both performance and robustness in comparison with the PID controller. The controller is very vital in secure communication, to increase the robustness of the RBF-based controller, in the second method the integral of the errors is also added to the RBF model makes the “RBF + error integral” neural (IRBFNN) controller. The unknown parameters of the latter controller are also obtained via PSO algorithm. For better comparison, an Optimal PID controller optimized by PSO is also used for secure communication. As the number of iterations was applied to chaotic map to reach the region corresponds to that text[6].

A simple one dimensional logistic map governed by the following equation

$$Xn+1 = bXn\,(1 - Xn),$$

where *b* is the gain and $Xn \in [0, 1]$.

Since the cipher texts are small integers, they are suitable to be transmitted through today's public digital networks. In order to avoid statistical and differential cryptanalysis, a random number is generated each time the chaotic trajectory has reached the desired region. If it is greater than a verge η, the current. The cipher text will be transmitted as number of iterations. Otherwise, the iteration will continue.

CHAOTIC ENCRYPTION

Bapista Theory

The use of chaotic systems for security or private communications has been a dynamic sector of research in the bygone few years. It depends on the particulars that Chaotic signals are usually noise-like and chaotic systems are very sensitive to initial condition. Rather than the equivalent protected communications that are relied on the synchronization of chaotic systems[7]. A chaotic cryptographic method that encrypts the message text as the number of iterations applied in the chaotic map in order to reach the region corresponds to that text.

A simple one dimensional logistic map governed by the following equation

$Xn+1 = bXn\ (1 - Xn)$,

where b is the gain and $Xn \in [0, 1]$.

Since the cipher texts are small integers, they are suitable to be transmitted through today's public digital networks. In order to avoid statistical and differential cryptanalysis, a random number is generated each time the chaotic trajectory has reached the desired region[7]. If it is greater than a threshold (verge) η, the current.

Number of iterations will be transmitted as cipher text.

Otherwise, the iteration will continue.

CHAOTIC ENCRYPTION BASED ON PARAMETER

Based on factor identification, a factor viewer is designed for a class of chaotic systems. The modulated signal (digital) in the factor will be recovered by the observer[10]. By selecting various different frequency signals as "zeroes" and "ones" a practical digital secure communication scheme is proposed by this parameter modulation method.

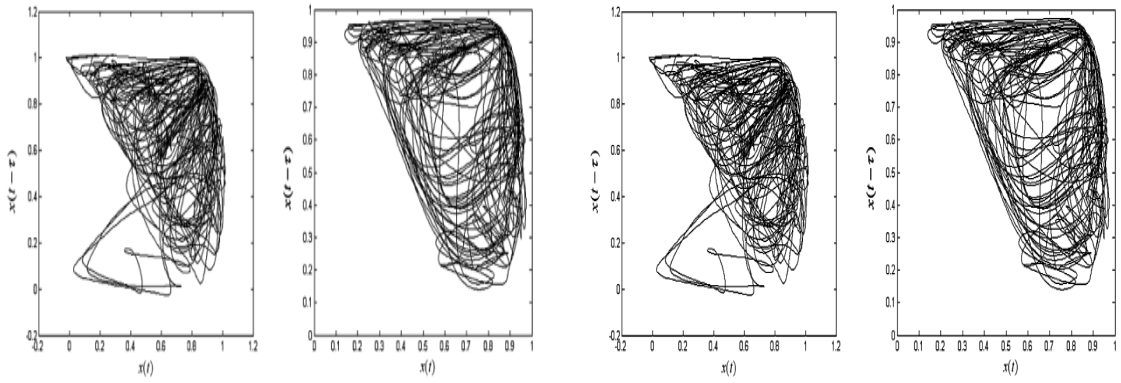

Figure 1: Strength of Chaotic Encryption

The strength of chaotic encryption varies in accordance with the number of commutative signals[11].

BLOCK DIAGRAM REPRESENTATION

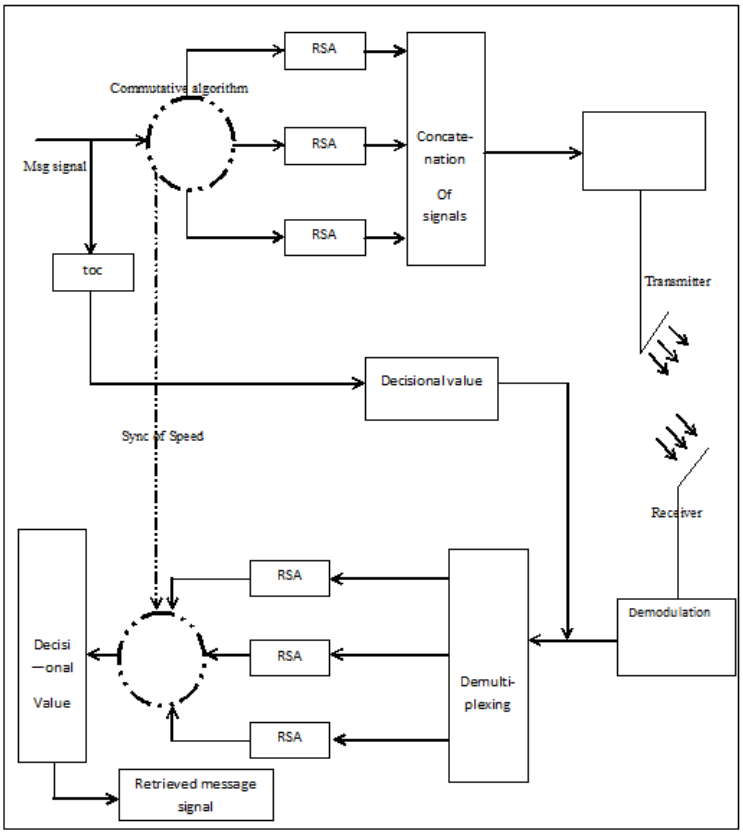

Figure 2: Block Diagram Representation of SCCE

BPSK: Binary phase shift keying or also known as BPSK which is change in phase of the signal according to binary inputs. BPSK is considered as the easiest form of PSK. There are two phases; each of them is 180 degrees apart. It requires more bandwidth. The transmitted power is lower.

Commutative Algorithm: In cryptography, the protocol known as three pass protocol is a framework to send messages which allow one party to securely send a message to a second party without the need to exchange or distribute encryption keys. This message protocol should not be confused with various other algorithms which use 3 passes for authentication.

RSA: RSA is an algorithm for cryptographic technique is a prime number based algorithm used to encrypt the message signal. The term RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. An applicant of RSA generates and then distributes the product of two large prime numbers, along with a support value, as their public key. The prime numbers used in the encryption should be kept top-secret. Anyone can use the public key to encrypt a message.

Overview of the project is to establish the secure communication between the user and the end user.

SIMULATION RESULTS

Simulation of the System

The implementation is done using Matlab. In this implementation one message signal is derived into three different signals using a commutative algorithm with different amplitude and frequency ranges and each signal is

encrypted based on the RSA algorithm. The original message signal is retrieved from the concatenated and modulated signal are done by using commutative algorithm.

The above implementations are done by using MATLAB.

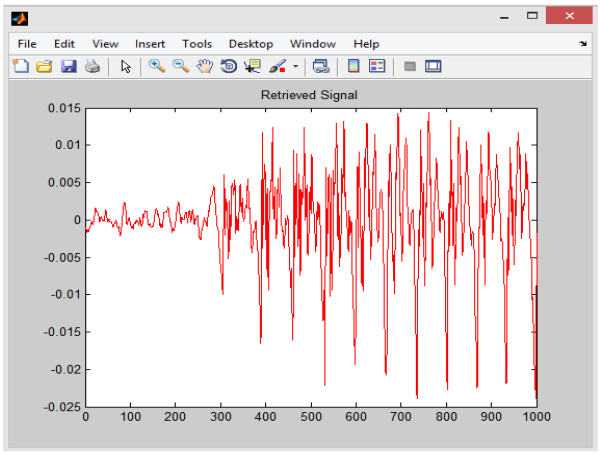

Figure 3: Representation of Original Message Signal

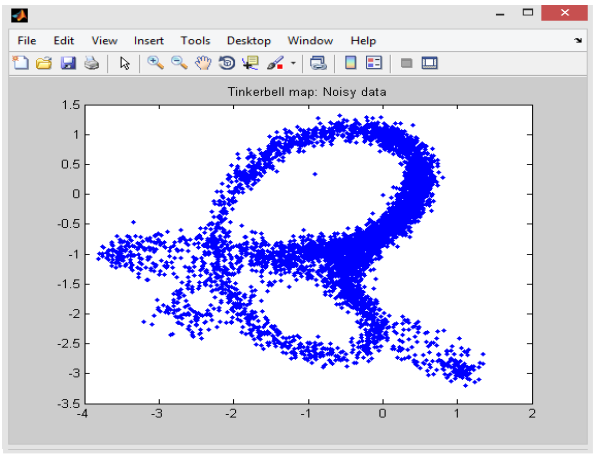

Figure 4: Representation of Chaotic Signal

Concatenation of Signals

The encrypted signals of the input signal is concatenated into a sequence of signal and the signal is modulated and transmitted through the communication channel. The concatenation of the signals (three signals) was done by multiplexing. The chaotic signal strength is increased by the factor called as Lyapnov exponent.

Mechanism of Encryption

In this mechanism each signal is assigned with different amplitude and time period levels. The signal is encrypted based on their random prime number generated by RSA algorithm. The three randomly assigned prime numbers were not equal ranges anywhere up to a predefined range of numbers.

Generating Chaotic Signals

The commutative algorithm samples the signal at a defined time interval and each signal is encrypted with the use of RSA algorithm and concatenated.

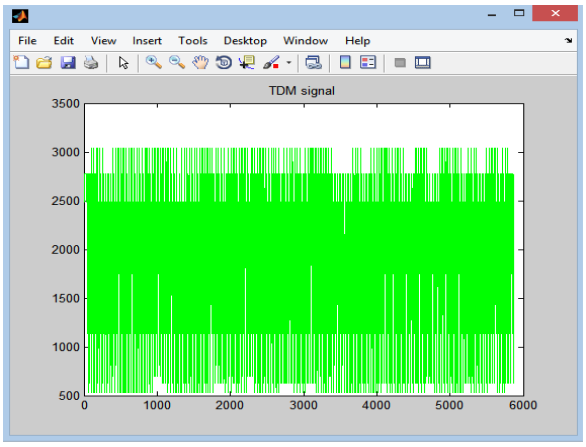

Figure 5: Representation of Multiplexed Signal

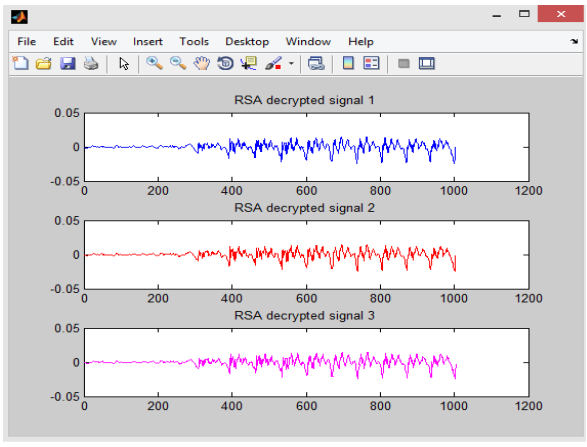

Figure 6: Representation of Decrypted Signal

The encrypted signals of the input signal are concatenated into a sequence of signal and the signal is modulated and transmitted through the communication channel.

Decryption of Signals

The decryption algorithm receives the signal from the communication channel and decrypts the signal based upon their amplitude and time period range. (Synchronization of speed through commutative algorithm).

The above steps are preceded by RSA algorithm.

IDS

The security of the signal over the communication channel is enhanced by implementing the Intrusion Detection System.

CONCLUSIONS

Thus the chaotic encryption method provides high security and ensures the data secrecy. The commutative principles and its speed synchronization determine the rate of efficiency of retrieval of original message signal.

FUTURE WORK

Future work of SCCE includes that; this research can also be influenced into other factors rather than the Lyapnov exponent to increase the strength of chaotic signal.

ACKNOWLEDGEMENTS

We express our sincere thanks to all the faculty members of Electronics and Communication department in the SNS College of Engineering, especially our Head of the Department and Our Project guide.

REFERENCES

1. Tanmoy Banerjee, Debabrata Biswas (2013) “Synchronization in hyperchaotic time-delayed electronic oscillators coupled indirectly via a common environment,” arXiv: 1303.5339v1 [online. CD] 21 Mar 2013.
2. Tannoy Banerjee, Debabrata Biswas, B.C. Sarkar (2012) “Complete and generalized synchronization of chaos and hyperchaos in a coupled first-order time-delayed system,” Nonlinear Dyn (2012), DOI 10.1007/s11071-012-0660-3, Springer Science+Business Media Dordrecht 2012.
3. Banerjee, T., Biswas, D., Sarkar, B.C. (2012) “Design and analysis of a first order time-delayed chaotic system,” Nonlinear Dyn (2012), DOI: 10.1007/s11071-012-0490-3, Published online12 June 2012.
4. Saptarshi Das, Indranil Pan, Shantanu Das, Amitava(2012), “Gupta generalized synchronization of chaos” (2012).
5. Slave chaos synchronization via optimal fractional order PIλDμ controller with bacterial foraging algorithm, Nonlinear Dyn (2012) 69:2193–2206**,** DOI 10.1007/s11071-012-0419-x Media B.V. 2012.
6. Seyyed Mohammad Reza Farschi, H. Farschi (2012) “A novel chaotic approach for information hiding in image,” Nonlinear Dyn (2012) 69:1525–1539, DOI 10.1007/s11071-012-0367-5, Springer Science+Business Media B.V. 2012.

7. Donato Cafagna, Giuseppe Grassi (2012) “Observer-based projective synchronization of fractional systems via a scalar signal: application of hyperchaotic Rössler systems,” Nonlinear Dyn (2012) 68:117–128, DOI: 10.1007/s11071-011-0208-y, Springer Science+Business Media B.V. 2011.

8. Mansour Sheikhan, Reza Shahnazi, Sahar Garoucy (2011) “Hyperchaos synchronization using PSO-optimized RBF-based controllers to improve security of communication systems,” Neural Comput & Applic, DOI 10.1007/s00521-011-0774-4, Springer-Verlag London Limited 2011.

9. DI-Yi Chen, Lin Shi, Hai-Tao Chen, Xiao-Yi Ma (2012) “Analysis and control of a hyperchaotic system with only one nonlinear term,” Nonlinear Dyn (2012) 67:1745–1752, DOI 10.1007/s11071-011-0102-7, Springer Science+Business Media B.V. 2011.

10. Cun-Fang (2010) “Feng Projective synchronization between two different Time-delayed chaotic systems using an active control approach,” Nonlinear Dyn (2010) 62: 453–459, DOI 10.1007/s11071-010-9733-3, Published online: 18 May 2010, Springer Science+Business Media B.V. 2010.

11. Cun-Fang (2010) “Feng Projective synchronization between two different Time-delayed chaotic systems using an active control approach,” Nonlinear Dyn (2010) 62: 453–459, DOI 10.1007/s11071-010-9733-3, Published online: 18 May 2010, Springer Science+Business Media B.V. 2010.