TELKOMNIKA, Vol. 11, No. 9, September 2013, pp. 5210~5217
ISSN: 2302-4046

Applications of Chaos Sequence in Intelligent Transportation System

Yao Zhang*[1,2], Licai Yang[1], Haiqing Liu[1], Lei Wu[1]
[1]School of Control Science and Engineeing, Shandong University, Jinan, 250061, China
[2]School of Mechanical, Electrical and Information Engineeing, Shandong University (Weihai), Weihai, 264209, China
Corresponding author, e-mail: zhangyao@sdu.edu.cn, yanglc@sdu.edu.cn, liuhaiqing0623@ 126.com, wulei-17@163.com

Abstract

Vehicular Ad-Hoc Network (VANET) is an essential technology to improve safety and efficiency of Intelligent Transportation System (ITS), it provides vehicle to vehicle as well as vehicle to roadside unit (RSU) wireless communications, so that on board unit (OBU) located in vehicles can share messages related to road traffic with not only other OBU in the same VANET but also transportation management centre depending on retransmission of RSU. It is very important to detect and transmit real time messages of road traffic condition in VANET. This paper presents two application schemes for VANET based on chaos sequence: traffic flow forecast and vehicle secret communications. The principles of these schemes are introduced separately, and performances are verified by theoretical analysis and simulation.

***Keywords**: ITS, VANET, chaos sequence, traffic flow forecast, secret communication, synchronization control, simulation*

1. Introduction

Vehicular Ad-Hoc Network (VANET) aims at achieving intelligent inter-vehicle communications and seamless Internet connectivity, it has been considered to be an essential technology to improve safety and efficiency of transportation, and becoming one of the most important parts of future intelligent transportation system (ITS). The ITS structure is shown in Figure 1, on board unit (OBU) located in vehicles is designated as a node to detect current road traffic conditions, and broadcast related information to neighboring vehicles by multiple hops through vehicle-to-vehicle communications. Meanwhile, vehicle-to-roadside unit (RSU) communications can provide high bandwidth links between OBU and Internet, so that messages related to road traffic safety can also be shared with remote users, transportation management centre and other VANTEs depending on RSU's retransmission. It is very important to collect and process real time traffic messages for improving efficiency of transport system. On the other hand, because the wireless channels in VANET are opened to public use, secret communications between vehicles are also very important to ensure information safety [1-3].

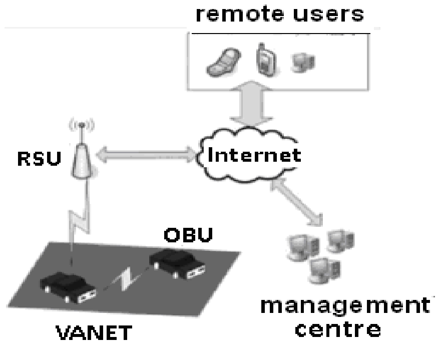

Figure 1. The Structure of Intelligent Transportation System

Received March 30, 2013; Revised June 7, 2013; Accepted June 19, 2013

This paper is organized as follows: In section 2, we present a traffic flow forecast model for VANET based on Logistic map, forecast accuracy is verified by theoretical calculation and actual data analysis. In section 3, we present a scheme for vehicular secret communications based on Logistic chaos sequence, the principle of synchronization control is discussed, and performance of our scheme is tested by MATLAB simulation. Finally, the useful conclusions and future research work are summed up in section 4.

2. Traffic Flow Forecast based on Logistic Map

2.1. Traffic Flow Forecast Model

Traffic flow is stochastic, but it has inner regularity in a short time interval. So it is an efficient way to forecast traffic flow during short time range by building forecast model based on chaos sequence [4, 5]. Define N_i denotes the number of vehicles detected by RSU between time interval i (i=1, 2, 3.....), it is a time series with uptrend. Let,

$$T_i = N_{i+1} / N_i \tag{1}$$

Fitting T_i into second-order polynomial by auto-regression, we have:

$$T_{i+1} = aT_i^{\,2} - bT_i + c \tag{2}$$

Defining d and X_i are intermediate variables, and let,

$$T_i = dX_i + \frac{(b+1) + \sqrt{(b+1)^2 - 4ac}}{2a} \tag{3}$$

Formula (2) can be transformed into:

$$X_{i+1} = adX_i^{\,2} + (1 + \sqrt{(b+1)^2 - 4ac})X_i \tag{4}$$

Let,

$$Y_i = \frac{-ad}{1 + \sqrt{(b+1)^2 - 4ac}} X_i, \quad \mu = 1 + \sqrt{(b+1)^2 - 4ac} \tag{5}$$

We have:

$$Y_{i+1} = \mu Y_i (1 - Y_i) \tag{6}$$

Formula (6) is a standard Logistic equation. The periodic orbit of Y_i is as shown as Figure 2, according to the theory of Logistic map [5], we can know that:

1) Y_i has two fixed points: $x_1 = 0$ and $x_2 = 1 - \frac{1}{\mu}$. If $0 \le \mu < 1$, x_1 is stable fixed point; if $1 \le \mu < 3$, x_2 is stable fixed point; if $\mu > 3$, Y_i becomes chaotic gradually.

2) Second iteration will add two fixed points: $x_3 = 1 + \mu - \frac{\sqrt{(\mu+1)(\mu-3)}}{2\mu}$ and $x_4 = 1 + \mu + \frac{\sqrt{(\mu+1)(\mu-3)}}{2\mu}$. If $0 \le \mu < 1$, x_1 is stable fixed point; if $1 \le \mu < 3$, x_2 is stable fixed point; x_3 and x_4 are unstable fixed points, but when $3 \le \mu < 1 + \sqrt{6}$, they are stable fixed points of second iteration.

So traffic flow N_i can be forecasted by following algorithm:

When real-time samples of traffic flow are obtained in each time interval:
Step 1: samples analysis.
Update forecast model according to formula (1) - formula (6).
Step 2: traffic flow forecast.
if $0 \le \mu < 1$ Y_i converges to 0.

if $1 \le \mu < 3$ Y_i converges to $(1 - \frac{1}{\mu})$.

if $3 \le \mu < 1 + \sqrt{6}$ {Y_i converges to $1 + \mu \pm \frac{\sqrt{(\mu+1)(\mu-3)}}{2\mu}$;

doubling forecast time interval. }

calculating convergence values of X_i, T_i by formula (5) and formula (3);
calculate forecast value N_i by recursion formula (1);
Step 3: delivering forecast results to management centre.

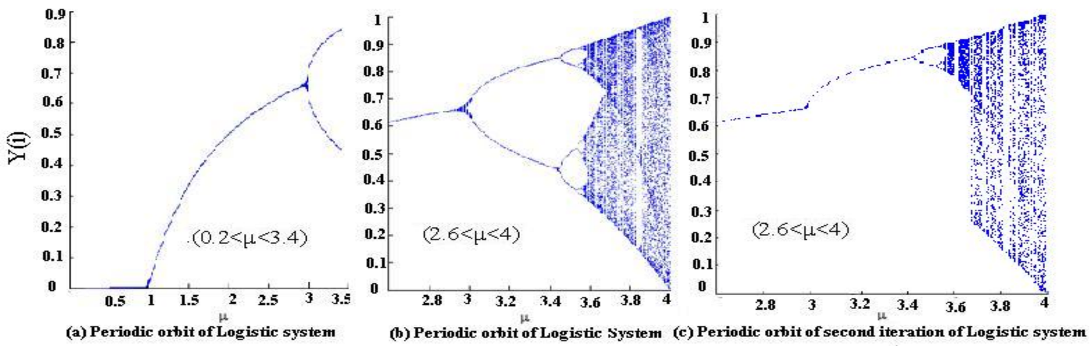

Figure 2. Periodic Orbit of Logistic Chaos Sequence

2.2. Data Process and Forecast Results Analysis

Table 1 is the samples of traffic flow at a crossroad in an urban transport system [4], the time interval unit is 5 minutes. Processing N_i with formula (1), we can get T_i as table 2. Fitting T_i into auto-regression second-order polynomial according to the principle of minimum mean-squared error, we have:

$$T_{i+1} = 0.83T_i^2 - 1.5T_i + 1.77 \tag{7}$$

Using formulas (3), (4) and (5), we can work out:

$$Y_{i+1} = 1.6112\, Y_i(1 - Y_i) \tag{8}$$

Because μ=1.6112, it is between 1 and 3, so Y_i converges to:

$$Y_\infty = 1 - \frac{1}{1.6112} = 0.3793 \tag{9}$$

X_i converges to:

$$X_\infty = \frac{-\mu}{ad} Y_\infty = \frac{-0.7363}{d} \tag{10}$$

T_i converges to:

$$T_\infty = -0.7363 + \frac{(1.5+1) + \sqrt{(1.5+1)^2 - 4\times 0.83 \times 1.77}}{2\times 0.83} = 1.1379 \quad (11)$$

Table 1. The Samples of N_i (start time: 7:30; time interval is 5 minutes)

Time	Ni	Time	Ni	Time	Ni	Time	Ni	Time	Ni
7:40	437	7:55	1063	8:10	1783	8:25	2593	8:40	3534
7:45	639	8:00	1321	8:15	2039	8:30	2934	8:45	3917
7:50	896	8:05	1500	8:20	2292	8:35	3236	8:50	4202

Table 2. The Calculation Results of T_i

Time interval	Ti	Time interval	Ti	Time interval	Ti	Time interval	Ti	Time interval	Ti
1	1.4622	3	1.1864	5	1.1355	7	1.1436	9	1.1313
2	1.4022	4	1.2427	6	1.1887	8	1.1241	10	1.1315

We forecast traffic flow after 8:30 using two methods: Logistic map by formula (11), auto-regression model by formula (7). The analysis results are shown in table 3. It is clear that

1) In general, forecast accuracy of Logistic map is better than auto-regression model.

2) Our traffic flow forecast scheme has better accuracy on short-range forecast, but with the increase of forecast time interval, forecast error increases. In order to improve forecast accuracy, forecast model should be updated dynamically according to the latest real time samples of traffic flow.

3) The value of μ has great influence on traffic flow. With the increase of μ, the convergence value of Y_i becomes smaller, it makes the uptrend of N_i decrease. The value of μ is related to *a, b* and *c* according to formula (2), so we can achieve optimized traffic flow trend by adjusting the values of *a*, *b*, *c* through reasonable transportation control measures.

Table 3. The Forecast Results of Ni using Two Analysis Methods

Time	Logistic map		auto-regression	
	forecast result	relative error	forecast result	relative error
8:35	3339	3.2%	3335	3.06%
8:40	3799	7.5%	3801	7.56%
8:45	4322	10.26%	4327	10.4%
8:50	4918	17.07%	4924	17.19%
8:55	5597	------	5602	------
9:00	6369	------	6374	------

3. Vehicle Secret Communications based on Chaos Sequence

3.1. Scheme of Vehicular Secret Communications in VANET

IEEE 802.11p is a new communication standard, which is designed for WAVE (Wireless Access in Vehicular Environments) to support VANET. 75MHz of licensed spectrum at 5.9GHz is divided into one control channel (CCH) and six service channels (SCHs), CCH is dedicated for broadcast of traffic safety messages, SCHs are dedicated for transmission of various application messages. Messages on SCHs can be transmitted using IPv6 protocol, WAVE application messages on CCH are transmitted using WSMP (Wave Short Message Protocol). In MAC layer, CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) algorithm is used for wireless channel competition. In order to supprot varying QoS requirements, messages are classified into different priority queues by EDCA (Enhanced Distributor Channel Access) mechansim. In physical layer, WAVE uses OFDM (Orthogonal Frequency Division Multiplexing) technology to split the signal into several narrowband channels to provide a data payload communication capability of 3 Mbps up to 27 Mbps. In order to reduce the effects of Doppler spread, 802.11p uses 10MHz frequency bandwidth, the double guard bands are used to reduces the Inter Symbol Interference (ISI) caused by multi-path in wireless channels, and making the signal more robust against effects of fading [2, 6, 7].

Wireless channels in VANET are opened to public use, so secret communications between vehicles are very important to ensure information safety. Because messages in VANET are burst, light-weight cipher can be used in vehicular secret communications. Secret communications can usually be achieved by encryption coding or scrambling technology [8, 9]. Figure 3 is the constitution of proposed VANET secret communication system, which is based on scrambling technology by Logistic chaos sequence. At information sending side, binary flow is segmented into data packets, the length of each packet is M bit. After chaos sequence X_n is transformed into M bit binary sequence U_i by quantization and coding, secret sequence T_i can be obtained by S_i (information sequence) adding U_i modulo 2. And then, T_i is modulated by OFDM, and be sent to wireless channel. At information receiving side, a series of reverse processing can restore information sequence (if has not information loss, R_i equals to S_i).

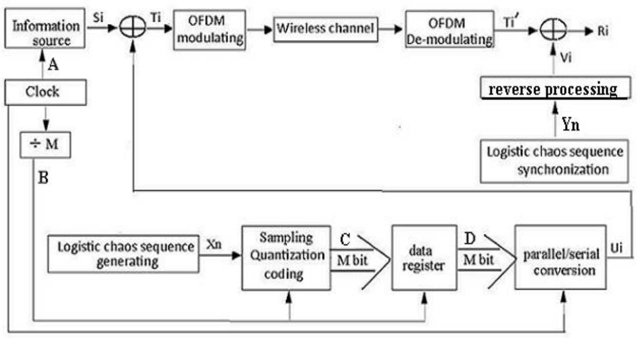

Figure 3. The constitution of secret communication system in VANET

In VANET secret communication system, because that chaos sequence is very sensitive to initial value, the periodic orbits of two identical chaos systems may become uncorrelated. So it is difficult to ensure synchronization of chaos sequences between sending side and receiving side. So far, many theories of synchronization control for chaotic sequences have been proposed [10-12], we present a straightforward method to perform synchronization control between Logistic chaotic sequence X_n and Y_n. Let,

$$\begin{aligned} X_{n+1} &= \mu_1 X_n (1 - X_n) \quad (3.6 < \mu_1 < 4) \\ Z_{n+1} &= \mu_2 Z_n (1 - Z_n) \quad (3.6 < \mu_2 < 4) \\ e_n &= \alpha X_n + \beta Z_n \\ e_{n+1} &= \mu e_n (1 - e_n) \quad (1 < \mu < 3) \end{aligned} \tag{12}$$

X_n and Z_n are all chaos sequences. Further more, we let,

$$Z_{n+1} = \mu_2 Z_n (1 - Z_n) + \xi_1 (X_n - Z_n) + \xi_2 [(\gamma + 1) X_n - Z_n)]^2 + 2\xi_2 \gamma X_n Z_n \tag{13}$$

We can get:

$$\begin{aligned} \alpha\mu &= \alpha\mu_1 + \beta\xi_1 \\ \alpha^2\mu &= \alpha\mu_1 - \beta\xi_2(\gamma+1)^2 \\ \mu &= \mu_2 - \xi_1 \\ \alpha\mu &= \xi_2 \end{aligned} \text{. and then, we have } \begin{aligned} \xi_1 &= \mu_2 - \mu \\ \xi_2 &= \frac{\mu_2(\mu_2 - \mu)}{\mu_2 - \mu_1} \\ \alpha &= \frac{\mu_2(\mu_2 - \mu)}{\mu(\mu_2 - \mu_1)} \\ \beta &= \frac{\mu_2(\mu - \mu_1)}{\mu(\mu_2 - \mu_1)} \end{aligned} \tag{14}$$

In this case, e_n converges to stable fixed point $e^* = 1 - \frac{1}{\mu}$. X_n and Z_n have linear relationship as $Z_n = \frac{1}{\beta}(e^* - \alpha X_n)$. Let $Y_n = \frac{1}{\alpha}(e^* - \beta Z_n)$, X_n and Y_n can keep synchronization commendably.

3.2. Simulation Analysis of Vehicular Secret Communication Scheme

Let μ=2, μ_1=3.9, μ_2=3.7. According to formula (14), we have ξ_1=1.7, ξ_2=31.45, α=-15.725, β=17.575, γ=0.002841, M=8. We build simulation model in MATLAB to verify presented VANET secret communication system. Figure 4 and Figure 5 are simulation results of synchronization control and data encryption. From simulation results, it is clear that Logistic sequence e_n is unstable at the beginning of simulation time. During this time, X_n and Z_n are asynchronous. When time interval n is more than 5, e_n converges to stable fixed point 0.5 accurately. From then on, synchronism is obtained between X_n and Z_n, Y_n and X_n are also synchronous. So ciphering and deciphering can keep consistent.

In order to estimate transmission performance, we also build simulation model of Frequency Shift Keying (FSK) modulating system in MATLAB/SIMULINK to transmit encrypted data sequence T_i. Two carrier frequencies of FSK are 400Hz (carrier frequency of data "1") and 800Hz (carrier frequency of data "0"), synchronous demodulation is used in receiver [13, 14]. Figure 6 is the architecture of FSK simulation system in MATLAB/SIMULINK, simulation results are shown in Figure 7. The simulation results show that information can be restored completely on receiving side if wireless channel is perfect (it means bit error rate is 0, i.e. T_i=T_i'), although there is transmission delay in some extent.

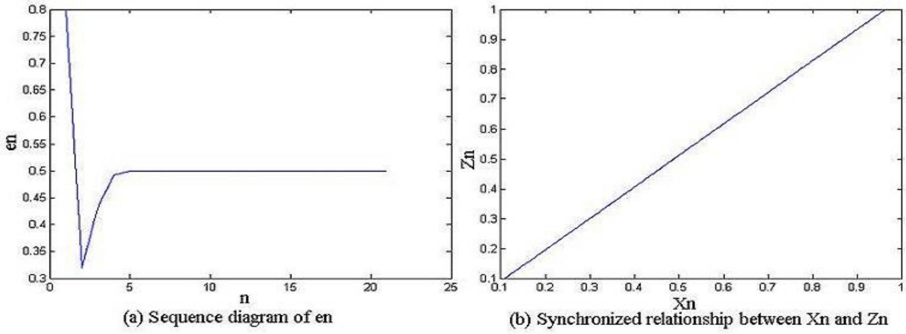

Figure 4. Synchronization Control between X_n and Z_n

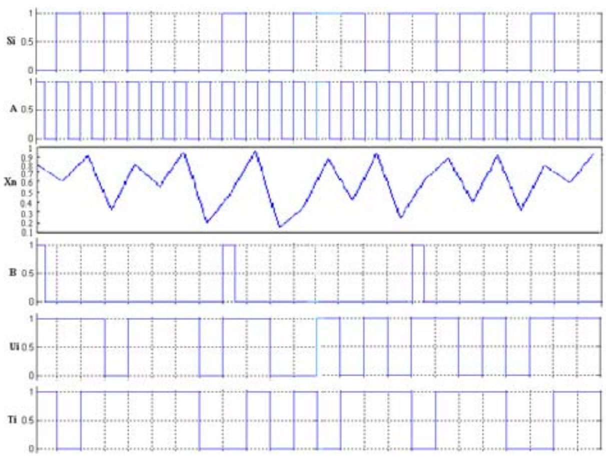

Figure 5. Simulation Process of Data Encryption in MATLAB Simulation

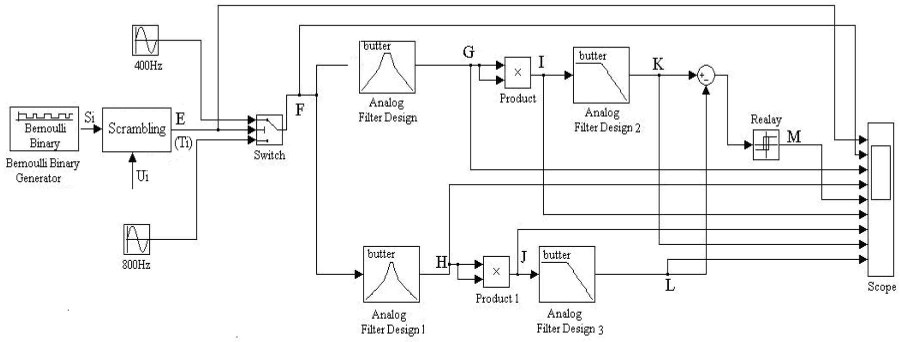

Figure 6. The Architecture of FSK Simulation System in MATLAB/SIMULINK

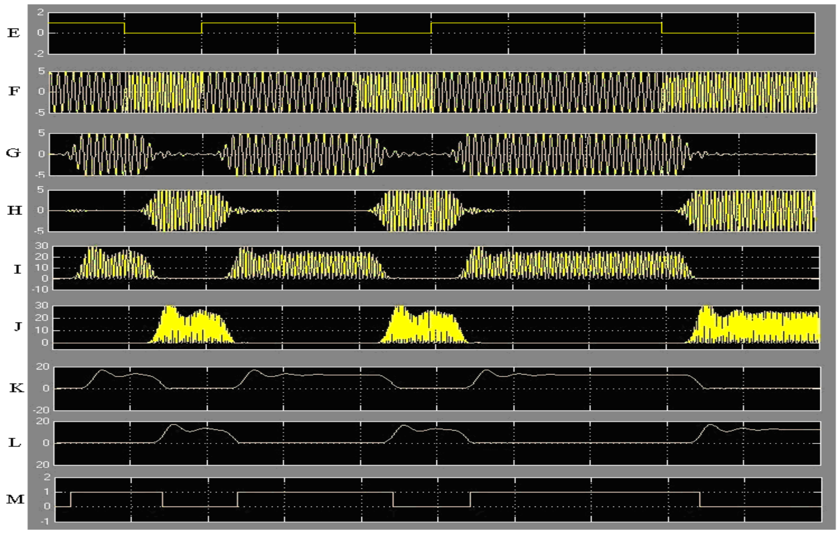

Figure 7. Simulation Results of FSK Communication System

4. Conclusion

In this paper, in order to improve the performance of VANET in Intelligent Transmission System, we present two application schemes based on Logistic chaos sequence: traffic flow forecast and VANET secret communications. For traffic flow forecast scheme, forecast model can be adjusted dynamically according to real time samples of traffic flow. Forecast accuracy is verified by theoretical calculation and actual data analysis, the analysis result appears that our scheme has more advantage on short time forecast of traffic flow. For VANET secret communications, we present a chaos sequence scrambling scheme, the principle of synchronization control is discussed in detail, the performance of this scheme is tested by MATLAB/Simulink simulation.

Our further research work includes studying on more accurate forecast model based on complex chaos sequence, frequency hopping secret communication technology used in VANET communication system based on OFDM, efficient channel assignment algorithm and priority control strategy in VANET.

Acknowledgements

This work is supported by Natural Science Foundation of Shandong Province of China (Grant No.ZR2010FM036), and National Natural Science Foundation of China (Grant No. 61174175).

References

[1] Chun Jing, Honggang Xu, Xing Wei, Zhifeng Luo, Shan He. Preliminary Implementation of Road-car Network Based on IEEE 802.11p /1609. *Application Research of Computers*. 2011; 28(11): 4419-4421.

[2] Amadeo Marica1, Campolo Claudia, Molinaro Antonellal. Enhancing IEEE 802.11p/ WAVE to Provide Infotainment Applications in VANETs. *Ad-Hoc Networks*. 2012; 10(2): 253-269.

[3] IEEE Std. P802.11p/D3.0. *Draft Amendment for Wireless Access in Vehicular Environments (WAVE)*. IEEE Press; 2007.

[4] Xinrong Liang, Zhiyong Liu, Deshan Sun, Zongyuan Mao. Application of Support Vector Machine to Prediction of Chaotic Systems. *Chinese Journal of Research on Computer Applications.* 2006; 23(5): 161-162.

[5] Qichang Zhang, Hongli Wang, Zhiwen Zhu et al. Theories and Applications of Bifurcation and Chaos. Tianjin: Tianjin University Press. 2005.

[6] Hendra Setiawan, Yuhei Nagao, Masayuki Kurosaki, Hiroshi Ochi. IEEE 802.11n Physical Layer Implementation on Field Programmable Gate Array. *Telkomnika*. 2012; 10 (1): 67-74.

[7] Serkan Oztürk, Jelena Mišic, Vojislav B Mišic. *Video Communications over IEEE 802.11p Network Using Single Channel Devices.* Proceedings of 7th International Wireless Communication and Mobile Computing Conference. Istanbul, Turkey. 2011; 1238-1243.

[8] Muhammad Aamir, Shabbir Mukhi. Algorithm to Detect Spurious Communications in Vehicular Ad hoc Networks. *International Journal of Information and Network Security*. 2013; 2(3): 239-244.

[9] Wampler David, Huirong Fu, Zhu Ye. *Security threats and Countermeasures for Intra-Vehicle Networks*. Proceedings of 5th International Conference on Information Assurance and Security. Xian, China. 2009; 153-157.

[10] Zhengyuan Xu, Liuxiao Guo, Rong Zhang. Generalized Synchronization in Complex Systems. Beijing: Beijing Normal University Press. 2012.

[11] Yuelin Du, Jingxian Zhang. The Performance of Synchronization Algorithm in Real-time OFDM-PON System. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10 (7): 1784-1794.

[12] Xiaolin Ren, Guangrui Hu, Zhenghua Tan. Synchronization of Discrete Chaotic Systems by Nonlinear Feedback Control. *Chinese Journal of Shanghai Jiaotong University*. 2001; 35(1): 105-107.

[13] Leon W Couch Ⅱ. Digital and Analog Communication Systems. Beijing: China Science Press. 2009.

[14] Yongan Huang, Wencheng Li, Xiaoke Gao. Application Example Simulations and High Efficiency Algorithm Development Using Matlab7.0/Simulink6.0. Beijing: Tsinghua University Press. 2008.