KEPCO Journal on Electric Power and Energy, Vol. 2, No. 4, December 2016

Microcontroller-based Chaotic Signal Generator for Securing Power Line Communication: Part I-A System View

전력선 암호화 통신을 위한 마이크로콘트롤러 기반 카오스 신호 발생기: 1부 - 시스템 뷰

Ala'aDdin Al-Shidaifat*†, Chamindra Jayawickrama*, Sunghyun Ji*, Van Ha Nguyen*††, Yoo-Jin Kwon**, Hanjung Song*†††
알라딘*†, 차민드라*, 지성현*, 응우웬 반하*††, 권유진**, 송한정*†††

* *Department of Nanoscience and Engineering, Inje University, 197 Inje-ro, Gimhae, Gyeongnam, 50834, Korea*
** *KEPCO Research Institute, Korea Electric Power Corporation, 105 Munji-ro Yuseong-gu, Daejeon 34056, Korea*
† *alaaddinsh@hotmail.com*
†† *nguyenha@oasis.inje.ac.kr*
††† *hjsong@inje.ac.kr*

Abstract

In this paper, the chaos-based secure scheme for power line communication is proposed for the first time. A digitalized chaotic generator based Lorenz system is utilized for generating nonlinear dynamic chaotic signal for masking the information signal instead of reported analog chaotic generators. A simple method of encryption and decryption is also given. In order to confirm the feasibility of the proposed scheme, the system is simulated using a simplified encryption/decryption method in Proteus. The gained results from simulation demonstrated that by using the chaos-based security method, the data can be encrypted and easily transmitted through the power line network efficiently.

Keywords: Power Line Communication, Chaos-based Security, Lorenz System, Chaos Signal, Secure Communication, Microcontroller

I. INTRODUCTION

Power line communication (PLC) is the usage of electrical power networks for communication purposes. Power line communication (PLC) has been the object of scientific research since the early 1970s in high voltage (HV) systems in the field of the management and control of the HV transmission networks [1]. Nowadays, most technical effort is concentrated on medium voltage (MV) and low voltage (LV) power line channels owning to the huge development of PLC in home as well as industrial applications, such as monitoring systems, remote control, emergency signals, and network management (since PLC is developed associated with the smart grid) [2]. This is because the PLC networks are inherently broadcast in nature and enables one to reach out to areas wider than those accessible by a typical telephonic and internet networks that results in a big reduction of the installation and maintenance cost as compared to the other mentioned counterparts which needs the base infrastructures [1]-[2][15].

In the modern world, predominant communication media is mostly using the internetworking. Since the internet is a public network, there is a high risk of transmitting data through the internet network because of the security threats are high and more critical [3]-[5]. With the PLC-based application, since the available equipment is in net-connected, the security, safety, and convenience service systems using narrow band communications are also critical. Therefore, there is also a necessity of secure data transmission methods while transmitting the data in the PLC networks.

In this paper, a new scheme of securing data for power line communication for the low voltage networks is proposed for the first time. The proposed system is based on a digitalized chaotic generator using a microcontroller unit and a simple amplitude modulation scheme for masking the information before it is transmitted on the power line networks. The rest of the paper is organized as follows: In the Section II, an overview about the system level of the proposed scheme in secure power line communication is described. The chaos-based generator using microcontroller units for masking the information which later utilize for high voltage PLC applications is also presented in this Section. Section III presents the results and discussions and several main points are concluded in Section IV.

II. SECURE POWER LINE COMMUNICATION SCHEME USING LORENZ-BASED CHAOTIC SYSTEM FOR MEDIUM VOLTAGE NETWORKS

A. The proposed chaos-based secure power line communication system

In the power distribution system, the power supply network is divided into three levels: High voltage network (110-380 kV), medium voltage networks (10-30 kV), and low voltage network (220 V in Korea). While the internet service is mostly developed

Manuscript received June 28, 2016, revised November 21, 2016, accepted November 23, 2016
ISSN 2465-8111(Print), 2466-0124(Online), DOI http://dx.doi.org/10.18770/KEPCO.2016.02.04.563

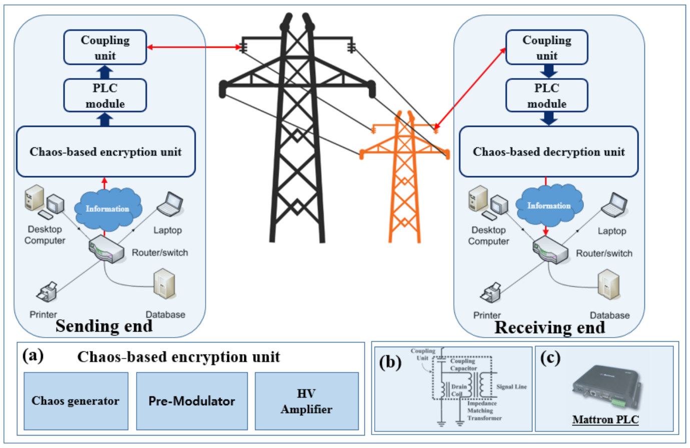

Fig. 1. The simplified diagram of the proposed chaos-based secure PLC system. (a) Chaos-based encryption/decryption unit, (b) Coupler [6][7], (c) PLC module.

over the medium voltage power lines because it covers largest areas, the power line communication has been widely used in low-voltage networks to control the housing equipment in specific areas [6].

Fig. 1 shows the simplified chaos-based PLC system for low voltage network. There is a transmitting end and receiving end. At the transmitting end, all of the equipment are connected to a router or a switch, and then signal path enters the chaos-based encryption unit which consists of a chaotic signal generator, a pre-modulator/demodulator and a HV (high voltage) amplifier. At this point, the information is firstly modulated with chaotic signal (which is generated by chaos generator) by using pre-modulator. At this stage, the information signal is encoded with chaotic mask signal in order to generate an encrypted counterpart. However, the voltage level here is not high enough that must be amplified by a HV amplifier in the same unit. Thereafter, the high frequency, encrypted signal enters the PLC module then coupled (injected) to the power line by capacitive couplers or inductive couplers as shown in Fig. 1(b) [6][7]. Power lines distribute the encrypted signal to the whole networks. At the receiving end, the encrypted signal will be decrypted through an inversed direction and finally this encrypted signal is decoded so that the original information can be recovered to be available at the end point. In the proposed system, the key lies on the chaos-based encryption/decryption unit. The coupling unit (coupler) can be designed based on the phase reported couplers [6][7] that transmits the signal coupling between two phase conductors. Besides, the proposed system is also compatible with the PLC modems on the market (Fig. 1(c)) that assures a cheap solution for secure communication using low voltage power line networks. The full design of the proposed system including the real hardware implementation will be presented at the second phase of our work. In the remained part of this paper, the chaos generator in chaos-based encryption/decryption unit is presented by using microcontroller unit which chaotic signal for masking the information.

B. Digitalized-chaos generator using Lorenz system for secure communication

Recently, secure communication systems employing chaos have attracted with significant interest. This is partly due to their high unpredictability and simplicity of implementation over conventional secure communications systems [8]. Because chaotic signals are typically broadband, noise-like and difficult to predict, they can be used in various contexts for masking information bearing waveform [9][10]. In the literature, there have been many reported about nonlinear systems which show the chaotic behavior at some certain conditions. Among these systems, Lorenz system demonstrates rich of nonlinear dynamics as well as can be easily implemented by electronic elements. In this research work, the chaotic generator for secure power line communication is based on Lorenz system which is described by a set of differential equations as following [11]-[14]:

$$\frac{dx}{dt} = p(y - x) \tag{1}$$

$$\frac{dy}{dt} = x(r - z) - y \tag{2}$$

$$\frac{dz}{dt} = xy - bz \tag{3}$$

where p, r and b are variables which can be used to control the dynamic behavior of the Lorenz system. A direct implementation of an electronic circuit is shown in Fig. 2. The operational amplifiers and associated circuitry perform the mathematical operations of addition, subtraction, and integration while the nonlinearity of Lorenz system is realized through analog multipliers. In order to obtain the chaotic behavior for secure communication purposes, the system parameters p, r and b must be assigned to some certain ranges. In fact, this is the simplest method to implement Lorenz system; however, this implementation presents one major disadvantage that is the controllability of its internal state (x, y, z) for chaos-based communication.

Because of this, a digitalized Lorenz system is proposed in this paper by using microcontroller unit. By using the microcontroller-based chaos generator, the chaotic signal can be easily obtained as in the analog implementation. Besides, the digitalized-chaos generator has its own advantage of easy controlling feasibility, ability to interface with digital systems, versatile and compact to be integrated on modules for consumer or industrial electronic appliances.

In order to implement the set of Lorenz equations in the digital-based system, the Lorenz system must be converted into a digitalized format. As reported in [4], we can re-write Lorenz system in terms of digital quantities by using the Euler method as following:

$$X(k+1) = X(k) + ts(p(Y(k) - X(k))) \tag{4}$$

$$Y(k+1) = Y(k) + ts(X(k)(r - Z(k)) - Y(k)) \tag{5}$$

$$Z(k+1) = Z(k) + ts(X(k)Y(k) - bZ(k)) \tag{6}$$

The implementation of the digitalized chaotic generator is presented in the next Section.

C. Encryption-decryption scheme in power line transmission

For securing the transmitted data, the information must be encrypted at the sending end as well as decrypted at the receiving

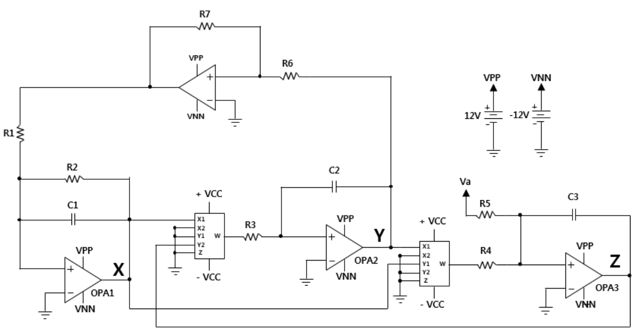

Fig. 2. Analogue circuit schematic diagram for chaos signal output; $x(t)$, $y(t)$ and $z(t)$ [3].

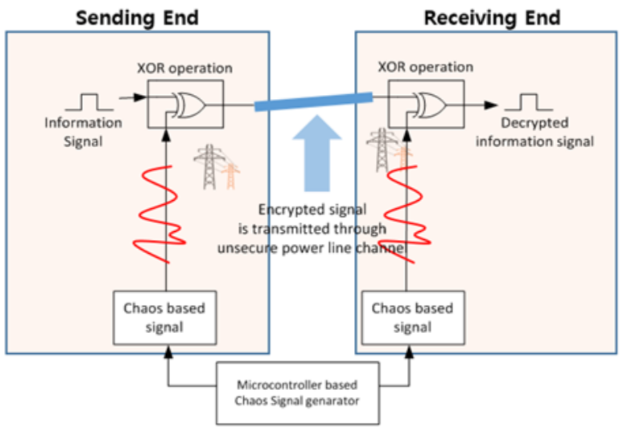

Fig. 3. Simplified block diagram of securing data by masking the information signal using chaotic signal.

end in order to recover the original data. The simple scheme for encrypting and decrypting data in chaos-based power line system is illustrated in Fig. 3. This scheme can be shortly described as follows: At the sending end, the information signal (data) is encrypted with the carrier chaotic signal which is generated from the microcontroller-based chaotic generator unit. After that, the signal will be coupled with the power line (as shown in Fig. 1) and then transmitted to the receiving end. At the receiving end, the encrypted signal is decrypted and the information signal is recovered.

III. RESULTS AND DISCUSSION

The digitalized-chaos generator for power line communication was realized using microcontroller 8-bit PIC18F4520 from Microchip for simplicity. The schematic of the chaotic generator along with encryption and decryption scheme is shown in Fig. 4 which can be divided into two blocks: The chaotic signal generator block and encryption/decryption block. As shown in Fig. 4, the chaotic generator is based on the microcontroller and digital to analog (DAC) circuits which are constructed using R-2D ladder topology. The algorithm of digitalized Lorenz system is shown in Fig. 5(a) and its equivalent source code using C language is illustrated in Fig. 5(b). The operation of the system can be summarized as following: Firstly, the algorithm of digitalized Lorenz equations is run by the microcontroller which outputs digital states of chaotic signals at the ports of the microcontroller. These digital chaotic states are then converted into analog chaotic signal through DACs and then encrypted with the information signal. After encoding, encrypted

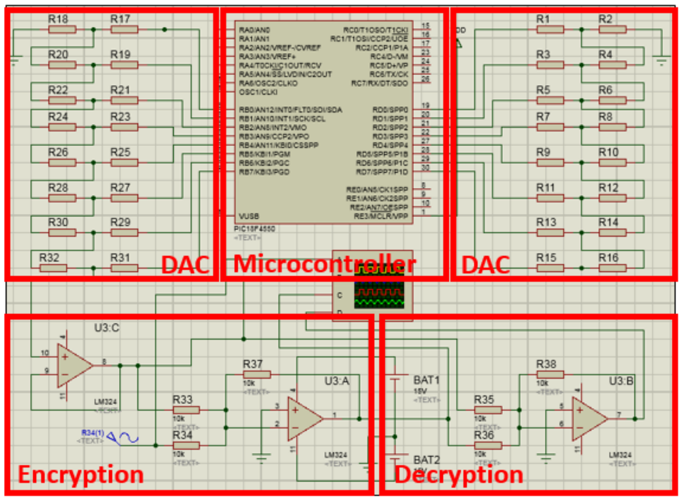

Fig. 4. Simplified scheme of chaos based communication system schematic diagram.

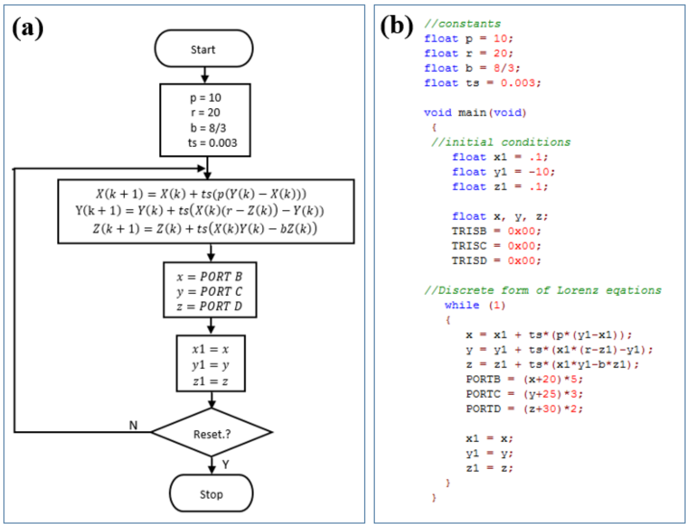

Fig. 5. (a) Flowchart of the Lorenz system algorithm. (b) Associated source code for Lorenz chaotic system using Proteus programming.

information signal and chaos signal both will be transmitted to receiving end. At the receiving end, a decryption process will be done and information signal will be recovered.

The simplified system illustrated in Fig. 4 was carried out by using Protues program. Firstly, the microcontroller-based chaotic generator using Lorenz system was simulated in order to confirm its expected chaotic outputs which later used for masking information signal of securing data in power line transmission. As mentioned before, the Lorenz chaotic system can show a rich of chaotic dynamic behavior at some specific conditions of the control parameters p, r and b. Here, the p and b were kept as constant and selected at 10 and 8/3, respectively, the parameter r was chosen to control the chaotic behavior of the chaos generator.

The chaotic generator was simulated at two typical cases with $r = 10$ and $r = 20$ which represented for an idle state and a working state, respectively. The outputs of the microcontroller-based chaotic generator under these conditions in form of time series, two-dimensional phase state as well as three-dimensional phase state are illustrated in Fig. 6, Fig. 7 and Fig. 8, respectively. As shown in these Figures, the dynamic state of microcontroller-based chaotic generator depends on the control factor r. If r value is increased, the number of peak states of time series of $x(t)$ (and

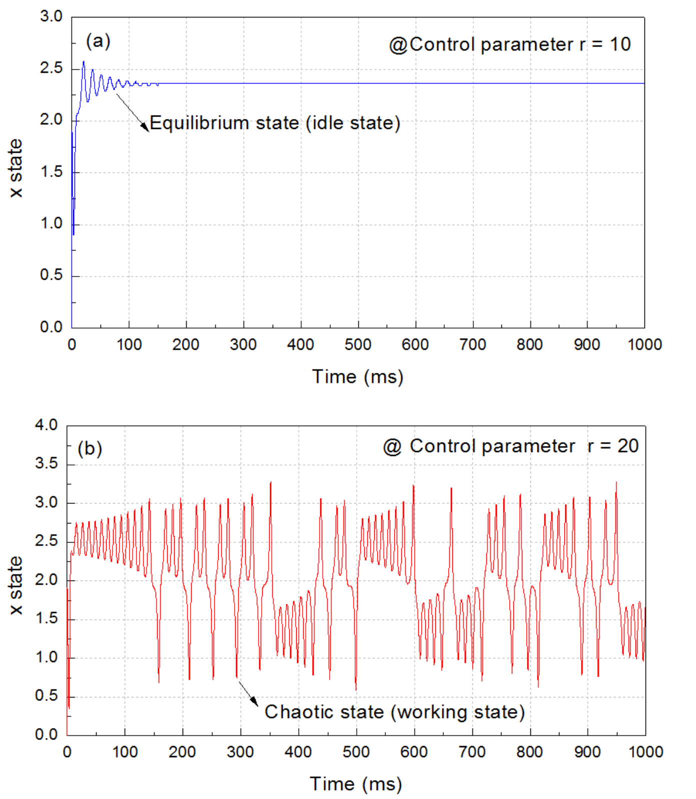

Fig. 6. Time waveform of x state at difference control values of r values. (a) Equilibrium state at r=10, (b) Chaotic stage at r=20.

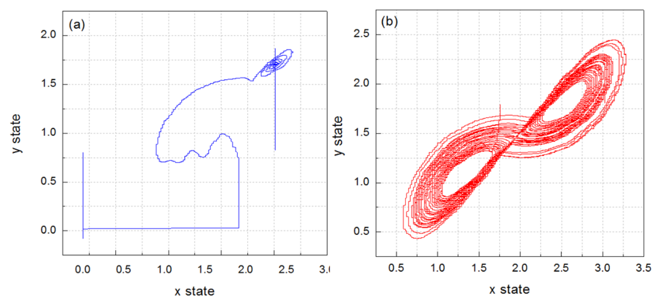

Fig. 7. Phase state between x and y of microcontroller-based Lorenz chaotic generator (a) at r=10, (b) at r = 20.

also $y(t)$ and $z(t)$ which are not shown) as well as the revolution of chaotic attractor will be increased and vice versa. Clearly, the microcontroller-based chaotic generator functions its expected behavior as in the Lorenz system-based chaotic generator using analogue circuit implementation which is reported in [4].

It should be noticed that, due to the limitation of resolution of the microcontroller (using 8-bit family) as well as the limitation of the resolution of the DAC units, the chaotic signal at the output contain high frequency noise. However, these issues can be solved by using an advanced microcontroller and DAC family with higher resolution such as 16-bit and 32-bit type. In addition, these chaotic signals can be filtered out and the analog-like chaotic signal can be easily obtained as obtained from the analogue Lorenz circuit implementation. Furthermore, for chaos-based power line communication, the proposed scheme is robust since the noise from digitalized Lorenz system does not effect on the performance of secure quality as well as the recovered information signal.

Finally, the encryption and decryption processes using generated digitalized chaotic signal are shown in Fig. 9 and Fig.

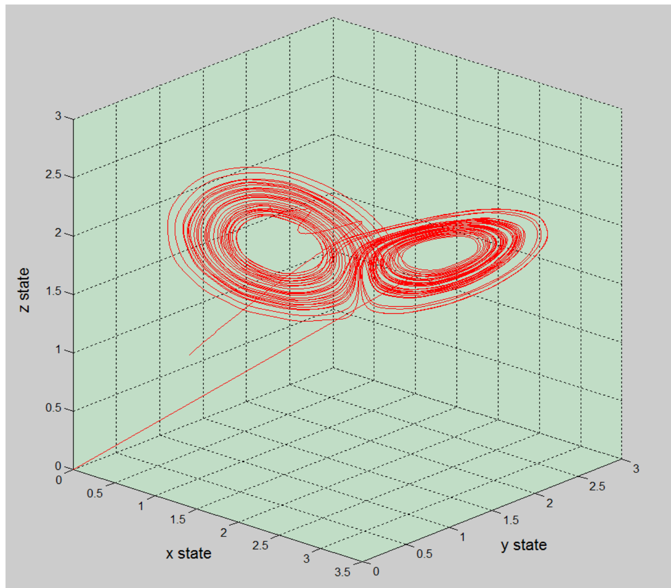

Fig. 8. 3-D chaotic attractor of x-y-z with r=20.

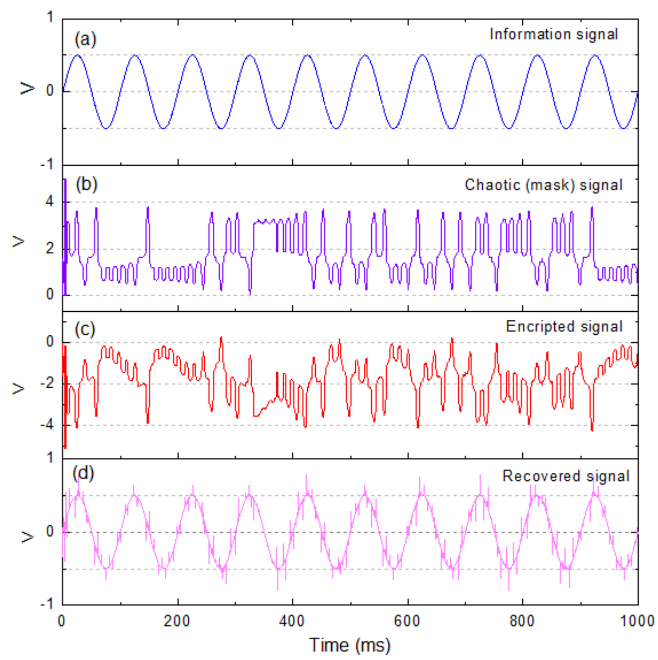

Fig. 9. Digital analysis waveform diagram. (a) Analogue information signal. (b) Chaos signal. (c) Encrypted signal. (d) Decrypted information signal.

10. In the simulation, the simple amplitude modulation (AM) technique was utilized for encrypting the message signal which is transmitted to the receiving end through the power transmission line. The information signal at the sending end was modeled by a sinusoidal signal (Fig. 9) and square wave pulses (Fig.10) respectively, represented for two different cases of analogue and digital signal transmissions. Both of the analog and digital signals are encrypted with a mask signal and then decrypted at receiving end. As mentioned before, there is some small noise remaining on the decrypted information signal; however, this can be eliminated using filters. Obviously, the scheme of using microcontroller for implementing and controlling chaotic system and the scheme of securing the data on power lines using the chaotic signal for masking the data are feasible. This means that the secure communication using power line can be implemented in practice.

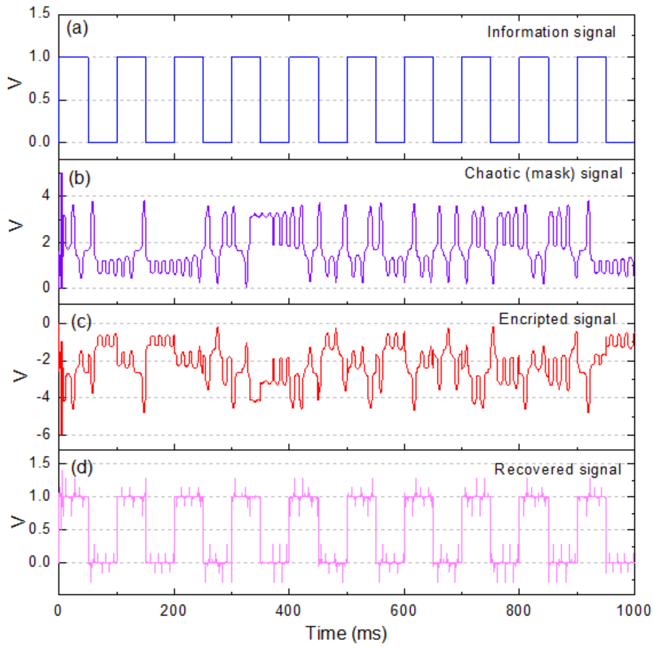

Fig. 10. Transmission scheme of digital information. (a) Digital information signal. (b) Chaos-mask signal. (c) Encrypted signal. (d) Decrypted information signal.

IV. CONCLUSION

In this paper, we have presented a new scheme of securing the information through the power line by using chaotic signal for the first time. The proposed system was simplified and modeled via a simple encryption/decryption method using chaotic signal as the mask signal for carrying the secured data on the power lines. The gained simulation results demonstrated that the chaotic system can be implemented on microcontroller unit, and the secure method for the information on the power line are feasible; therefore, the proposed scheme can be used effectively for ensuring security and privacy in commercial consumer electronics products in the power line communication stage.

ACKNOWLEDGEMENT

This research was supported by Korea Electric Power Corporation through Korea Electrical Engineering & Science Research Institute. (grant number: R15XA03-66)

REFERENCES

[1] Cataliotti, A., Daidone, A., Giovanni, T., "Power line communication in medium voltage systems: Characterization of MV cables", IEEE Trans. on Power Delivery, Vol. 23, No. 4, 2008. pp. 1896-1902.

[2] Ferreira, H. C., Lampe, L., Newbury, J., Swart, T. G., “Communication: Theory and Applications for Narrowband and Broadband Communications over Power Lines”, 2010.

[3] Murali, K., Yu, H., Varadan, H., Leung, H., "Secure communication using a chaos based signal encryption scheme", IEEE Trans. on Consumer Electronics, Vol. 47, No. 4, 2001, pp. 709-714.

[4] Chiu, R., Mora-Gonzaleza, M., Lopez-Mancillaa, D., "Implementation of a chaotic oscillator into a simple microcontroller", International Conference on Electronic Engineering and Computer Science, Vol. 4, 2013, pp. 247-252.

[5] Han, C., Yu, S., Wang, G., "A sinusoidally driven Lorenz system and circuit implementation", Mathematical Problems in Engineering, Vol. 2015, No. 706902, 2015, pp. 1-11.

[6] Papadopoulos, T., Batalas, B., Radis, A., Papagiannis, G., "Medium voltage network PLC modeling and signal propagation analysis", IEEE International Symposium on Power Line Communications and Its Applications, 2007, pp. 284-289.

[7] Lee, J., Park, Y., Kwon, S., Lee, D., Jeon, Y., "High data rate Internet service over medium voltage power lines", International Symposium on Power Line Communications and Its Applications, 2005, pp. 405-408.

[8] Huang, G., Zhou, Y., "Circuit simulation of the modified Lorenz system", Journal of Information and Computational Science, Vol. 10, No. 15, 2013, pp. 4763-4772.

[9] Radwan, A., Soliman, A., Sedeek, A., "MOS realization of the modified Lorenz chaotic system", Chaos, Solitons and Fractals, Vol. 21, No. 3, 2003, pp. 553-561.

[10] Huai-qing, X., Jian-kui, P., Zhen-qian, W., Ping, H., Li, Z., "A hyperchaotic Lorenz system circuit simulation and synchronization", Vol. 47, No. 5, 2011, pp. 120-125.

[11] Alsafasfeh, Q., Al-Arni, M., "A new chaotic behavior from Lorenz and Rossler systems and its electronic circuit implementation", Circuits and Systems, Vol. 2, No. 2, 2011, pp. 101-105.

[12] Hewlett, J., Wilamowski, B., "SPICE as a fast and stable tool for simulating a wide range of dynamic systems", International Journal of Engineering Education, Vol. 27, No. 2, 2011, pp. 217–224.

[13] Hrubos, Z., Gotthans, T., Petrzela, J., "Electronic experiments with dynamical model of thermostat System", Elektrorevue, Vol. 3, No. 1, 2012, pp. 65-70.

[14] Elwakil, A., Kennedy, M., "Chua's circuit decomposition: a systematic design approach for chaotic oscillators", Journal of the Franklin Institute, Vol. 337, No. 2-3, 2000, pp. 251-265.

[15] IEEE Guide for Power Line, IEEE Standards - 643, Jun. 8, 2005.