무손실 전송선로를 가진 카오스 회로에서의 카오스 비밀통신

배 영 철

여수대학교 전기공학과

Chaos Secure Communication with Lossless Transmission Line of Chaos Circuit

Young-chul Bae

Nat'l Yosu University

E-mail : ycbae@yosu.yosu.ac.kr

Abstract

Chua's circuit is a simple electronic network which exhibits a variety of bifurcati on and attractors. The circuit consists of two capacitors, an inductor, a linear resistor, and a nonlinear resistor.

In this paper, a transmitter and a receiver using two identical Chua's circuits are proposed and a secure communications of lossless transmission line are investigated. A secure communication method in which the desired information signal is synthesized with the chaos signal created by the Chua's circuit is proposed and information signal is demodulated also using the Chua's circuit.

The proposed method is synthesizing the desired information with the chaos circuit by adding the information signal to the chaos signal in the lossless transmission system.

1. 서 론

최근에 카오스 현상에 대한 관심이 물리학, 화학, 생물학, 공학 등에서 높아지고 있으며 이에 대한 응용이 활발하게 진행되고 있다.. Chua는 간단한 전자 회로로 카오스 현상이 존재함을 증명하였다. Chua 회로는 매우 단순한 자율, 3차계 시스템으로 가역성을 가지며 1개의 비선형 소자인 3 구분 선형 저항(3 - segment piecewise - linear resistor)과 4개의 선형 소자인 (R, L, C_1, C_2)로 구성되는 발진회로다.

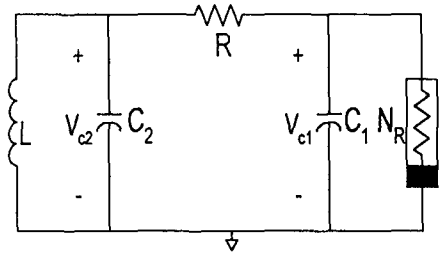

그림 1. Chua 회로

Matsumoto에 의해 제안된 Chua 회로[1]를 그림 1에 나타냈으며 상태방정식은 다음과 같이 표시할 수 있다.

$$C_1\frac{dv_{C_1}}{dt} = G\,(v_{C_2} - v_{C_1}) - g(v_{C_1})$$

$$C_2\frac{dv_{C_2}}{dt} = G\,(v_{C_1} - v_{C_2}) + i_L \qquad (1)$$

$$L\frac{di_L}{dt} = -v_{C_2}$$

여기서 $G = 1/R$, $g(\cdot)$는 식 (2)와 같이 표현되는 3구분 선형 함수 (3- segment piecewise-linear function) 이며 그림 2에 나타내었다.

$$g(v_R) = m_0 v_R + \frac{1}{2}(m_1 - m_0)[|v_R + B_P| - |v_R - B_P|] \qquad (2)$$

여기서 m_0 는 외부 영역의 기울기, m_1 은 내부 영역의 기울기, $\pm B_P$ 는 break-point이다.

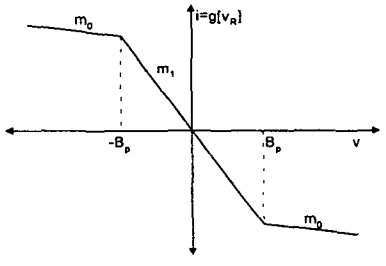

그림2. 비선형 저항의 전압 전류 특성

카오스 암호화에 관한 이론은 주로 채널을 이상적인 채널로 보고 적용한 경우가 대부분이며 이는 실제 선로를 고려하지 않아 적용 상의 문제점이 있다. 이에 본 연구에서는 동일한 2개의 Chua 회로 사이에 무손실 등가 전송선로를 둔 카오스 암호화 관하여 연구하였으며 복조부에서 전류 검출기를 두어 복조한 신호와 정보 신호를 비교하고 선로 중간에서 도청하여 정보 신호와 비교함으로써 암호 통신에 대한 안전성을 검토하였다.

2. 관계이론

2.1 등가 무손실 전송선로를 가진 Chua 회로

구분 선형 소자를 가진 Chua 회로의 LC 공진기를 한쪽이 단락된 무손실 전송선로로 치환하면 그림 3과 같은 회로를 얻을 수 있다.

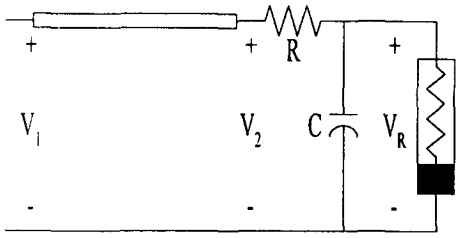

그림 3. 전송 선로를 가진 Chua 회로

Branin[4]는 무손실 전송선로의 과도 해석을 위한 특성곡선법을 제안하였다. 그림 4와 같은 전송 선로의 특성 방정식은 다음과 같이 표시된다.

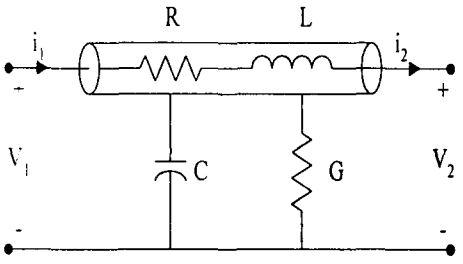

그림4. 전송 선로

$$L\frac{\partial i}{\partial t}+Ri+\frac{\partial e}{\partial x}=0 \qquad (3)$$

$$C\frac{\partial e}{\partial t}+Ge+\frac{\partial i}{\partial x}=0 \qquad (4)$$

여기서 $e(x,t)$와 $i(x,t)$는 시간 t에서 선로 x점의 전압과 전류, R, L, C, G는 단위 길이당의 저항, 인덕턴스, 커패시턴스, 컨덕턴스를 나타낸다.

특성곡선에서 정의된 $dx/dt=1/\sqrt{(LC)}$과 $dx/dt=-1/\sqrt{(LC)}$를 사용하여 식(3)과 식 (4)를 계산하면 다음식과 같은 상미분 방정식을 유도할 수 있다.

$$\sqrt{\frac{L}{C}}di+(Ri+\sqrt{\frac{L}{C}}\ G\ e)dx+de=0 \qquad (5)$$

$$-\sqrt{\frac{L}{C}}di+(Ri-\sqrt{\frac{L}{C}}\ G\ e)dx+de=0 \qquad (6)$$

식(5)는 $dx/dt=1/\sqrt{(LC)}$ 일 때 얻어지며 진행파 특성을 가지고 식(6)는 $dx/dt=-1/\sqrt{(LC)}$ 일 때 얻어지며 반사파 특성을 가진다.

식(5)와 (6)에서 무손실 전송 선로인 경우 R=0, G=0이므로 다음과 같은 식으로 정리할 수 있다.

$$\Delta e=-Z_0\Delta i \qquad (7)$$

$$\Delta e=+Z_0\Delta i \qquad (8)$$

여기서 $Z_0=\sqrt{L/C}$ 이며 선로의 특성 임피던스, Δe는 주어진 선로에서의 임의의 두점간의 전압차, Δi는 전류차를 나타낸다.

전송선로의 길이를 d라고 하고 일단에서 다른 일단으로의 파의 지연 시간을 $\tau=\sqrt{LC}d$ 라 놓으면 식(9),(10)과 같은 전압 방정식을 세울 수 있다.

$$e(d,t)=-Z_0i(d,t)+[e(0,t-\tau)+Z_0i(0,t-\tau)] \qquad (9)$$

$$e(0,t)=+Z_0i(0,t)+[e(d,t-\tau)-Z_0i(0,t-\tau)] \qquad (10)$$

식(9)와 식(10)은 입사파와 반사파 전압원을 이용하여 다음과 같은 수식으로 정리 할 수 있다

$$e(d,t)=-Z_0i(d,t)-e_2(0,t-\tau) \qquad (11)$$

$$e(0,t)=+Z_0i(0,t)-e_1(d,t-\tau) \qquad (12)$$

여기서

$$e_2(0,t)=-[2e(0,t)+e_1(d,t-\tau)]$$

$$e_1(d,t)=-[2e(d,t)+e_2(0,t-\tau)]$$

이다.

식(11)과 식(12)의 등가 회로를 그림 5에 나타내었다.

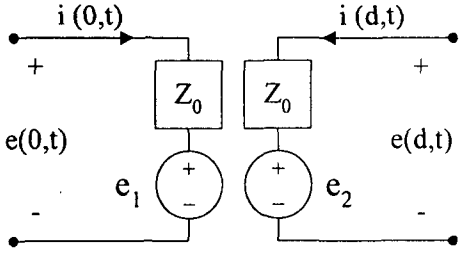

그림 5. 전송 선로의 특성 모델

그림 4의 전송선로는 그림 5와 같이 등가 변환되므로 전송선로를 가진 그림3의 Chua 회로는 그림 6과 같은 새로운 등가회로로 변환할 수 있다.

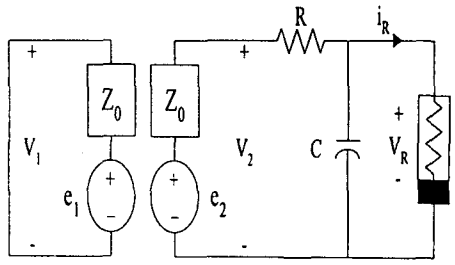

그림 6. 전송 선로를 가진 Chua 회로의 등가회로

2.2 무손실 전송선로를 가진 Chua 회로에서의 카오스 암호 통신

동일한 Chua 회로 2개를 송신부와 수신부로 놓고 그 사이에 등가 무손실 전송 선로를 가진 카오스 회로에서의 동기화 회로를 그림7에 나타내었다.

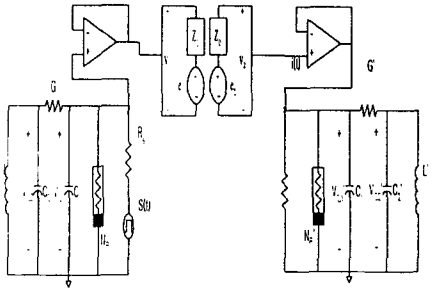

그림7. 등가 무손실 전송선로를 가진 카오스 암호통신 회로

그림 7은 동일한 2개의 Chua 회로에서 percora 와 Caroll이 제시한 구동 동기 이론을 적용하여 동기화를 이루고 정보 신호를 벡터장으로 카오스 신호와 합성하였다.

그림 7의 등가 전송 선로를 가진 동기화 회로의 상태방정식을 다음식과 같다.

송신부의 상태방정식

$$C_1\frac{dv_{c_1}}{dt} = G(v_{c_2}-v_{c_1}) - g(v_{c_1}) + \frac{e(t)-v_{c_1}}{R_s}$$
$$C_2\frac{dv_{c_2}}{dt} = G(v_{c_1}-v_{c_2}) + i_L \qquad (7)$$
$$L\frac{di_L}{dt} = -v_{c_2}$$

등가 무손실 전송선로부의 상태방정식

$$e_{1(t)} = 2v'_{c_1} - e_2\,(t-\tau) \qquad (8)$$
$$e_{2(t)} = 2v_{c_1} - e_1\,(t-\tau)$$

수신부의 상태방정식

$$C_1'\frac{dv_{c_1}'}{dt} = G'(v_{c_2}'-v_{c_1}') - g(v_{c_1}') - \frac{v_{c_1}'}{R_s} + i(t)$$
$$C_2'\frac{dv_{c_2}'}{dt} = G'(v_{c_1}'-v_{c_2}') + i_L' \qquad (9)$$
$$L'\frac{di_L'}{dt} = -v_{c_2}'$$

동기화 조건은 $v_{c_1}(t)=v_{c_1}'(t)$이 되는 것이다.

식(7)의 첫 번째 수식으로부터 정보 신호 $e(t)$를 구하고

$$e(t) = R_s[\,C_1\frac{dv_{c_1}}{dt} - G(v_{c_2}-v_{c_1}) + g(v_{c_1}) + \frac{v_{c_1}}{R_s}\,] \qquad (10)$$

식 (9)의 첫 번째 수식으로부터 전류 신호 $i(t)$를 구하여

$$i(t) = [\,C_1'\frac{dv_{c_1}'}{dt} - G'(v_{c_2}'-v_{c_1}') + g(v_{c_1}') + \frac{v_{c_1}'}{R_s}\,] \qquad (11)$$

동기화 조건 ($v_{c_1}(t)=v_{c_1}'(t)$) 를 대입하면 복조된 전류 신호 $i(t)$는

$$i(t) = \frac{e(t)}{R_s} \qquad (12)$$

로 되어 입력 정보 신호에 비례함을 알 수 있다.

식 (12)의 전류 $i(t)$를 검출하기 위한 회로를 그림 8과 같이 구성하였다.

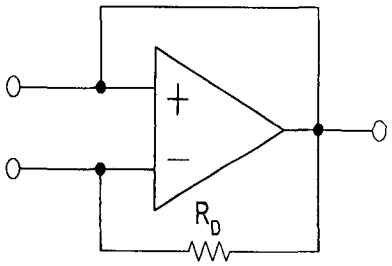

그림 8. 전류 검출기

본 논문에서는 그림 7의 무손실 전송선로에서 암호화 통신 회로에 그림 8의 복조회로를 추가하고 그림의 저항 소자 R_D = 2.8[$K\Omega$], R_s=33[$K\Omega$]를 적용했을 때의 시뮬레이션을 행하였다.

2.3 시간 지연 동기화에 의한 카오스 암호화 통신

본 논문에서는 폭넓은 주파수 분포를 가진 구형파 정보 신호를 대상으로 성능을 검토하기 위하여 그림 9과 같은 크기 -50[mV]~+50[mV], 주기 5[ms] 인 구형파 신호를 인가하였다.

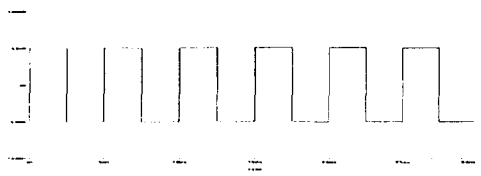

그림 9 구형파의 정보 신호

그림10은 구형파인 정보 신호와 반송파인 카오스 신호를 합성한 신호를 나타내었다. 구형파인 정보 신호가 완전히 반송파의 신호에 숨겨져 있음을 확인할 수 있다. 따라서 정보 은폐가 가능하다.

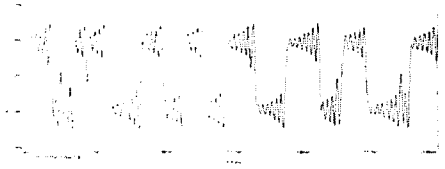

그림10, 정보 신호와 카오스 신호의 합성 신호

그림 11은 선로 중간에서 도청한 신호를 나타낸다. 도청된 신호가 구형파와 다른 신호로 중간에서 도청하여도 의미가 없음을 확인할 수 있다.

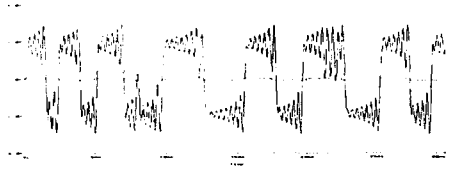

그림 11. 도청 신호

그림 12는 그림 8의 전류 검출기를 이용하여 복원한 복원된 신호를 나타내었다.

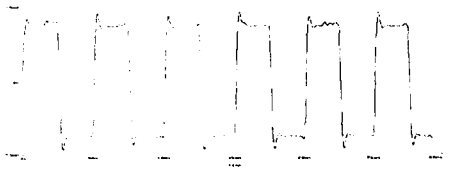

그림 12. 복원 신호

그림13은 정보 신호와 복원된 신호를 비교한 그림이다. 완전하게 복원되었음을 확인할 수 있다.

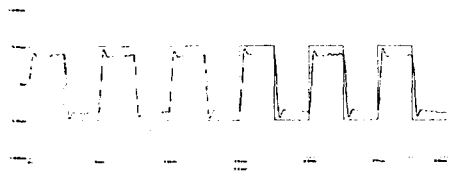

그림 13. 정보 신호와 복원 신호의 비교

3. 결 론

본 연구에서는 두 개의 동일한 Chua 회로에 무손실 전송선로를 두어 등가 전송로를 구성한 후 구동 동기 이론을 적용하여 암호화 통신을 행하였다. 무손실 전송 선로 가진 Chua 회로의 카오스 동기화는 전송 선로의 L과 C 영향에 의한 시간 지연이 있지만 완벽하게 정보 신호가 복호됨을 확인할 수 있었다.

[참 고 문 헌]

[1] T. Matsumoto, "A Chaotic Attractor from Chua's circuit", IEEE Trans. on Circuit and System, vol. CAS-31, pp. 1055 - 1058, 1984.

[2] 배영철, 고재호, 임화영, "Chua 회로에서의 Bifurcation과 Attractor", 대한전기학회 하계 학술대회 논문집, pp..664 - 666, 1995.

[3] 배영철, 고재호, 임화영, "구분 선형 함수의 최적 구현에 관한 연구", 한국자동제어학술 회의 논문집, pp. 370 - 373, 1995.

[4] 배영철, 고재호, 임화영, "Chua 회로에서의 파라미터 변화에 의한 Period-doubling과 Bifurcation에 관한 연구", 한국 자동제어 학술 회의 논문집, pp. 482 - 485, 1995.

[5] L. Kocarev, K. S. Halle, K. Eckert and L. O. Chua, " Expermental Demonstration of Secure Communication via Chaotic Synchronization" Int. J. Bifurcation and Chaos, vol. 2, no. 3, pp. 709-713, 1992.

[6] K. S. Halle, C. W. Wu, M. Itoh and L. O. Chua, " Spread Spectrum Communication through Modulation of Chaos " Int. J. Bifurcation and Chaos, vol. 3, no. 2, pp. 469-477, 1993

[7] F. H. Branin, Jr, "Transisent Analysis of Lossless Tranmission Lines". Proc. IEEE, vol.55, pp. 2012 - 2013, 1967.

[8] A. N. Sharkovsky, "Chaos from a Time-delayed Chaos Circuit", IEEE Trans. on Circuit and System, vol. CAS-40, pp. 781 - 783, 1993.

[9] L. Kocarev and Z. Tazev, "Analytical Description of a Fractal Set Generated by the Time-Delayed Chua's Circuit", International Journal of Bifurcation and Chaos, vol. 4, pp. 1639 - 1643, 1994.

[10] X. Rodet, "Models of Musical Instruments from Chua's Circuit with Time-Delay", IEEE Trans. on Circuit and System, vol. CAS-40, pp. 696-701, 1993.