카오스 회로의 암호 통신

배영철

Secure Communication of Chaos Circuit

Bae Young-Chul
Dept. of Electrical Eng. Nat'l Yosu Univ.

Abstract - Chua's circuit is a simple electronic network which exhibits a variety of bifurcation 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 equivalent T type wire secure communications 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 wire 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.

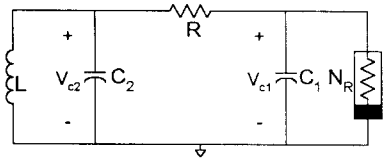

그림 1. Chua 회로
Fig. 1. Chua's circuit

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

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

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

$$L\frac{di_L}{dt} = -v_{C_2} \qquad (1)$$

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.

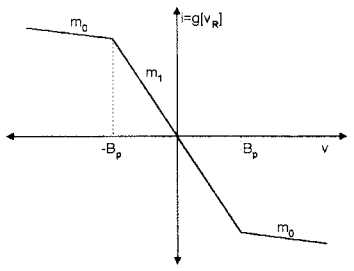

그림2. 비선형 저항의 전압 전류 특성
Fig.2. v-i characteristic of nonlinear resistor

본 논문에서는 T형 등가 전송 선로를 동일한 Chua 회로 사이에 놓고 정보 신호와 카오스 신호를 합성하였으며 수신된 통신 신호에서 정보 신호와 카오스 신호를 분리하는 복조 방법은 카오스 신호에만 동기하는 회로를 구성하고 그 회로에 유입하는 전류 신호를 검출하는 방법으로 구현하였으며 일반 필터링에 의한 복조 결과와 비교 검토하였다.

2. 본 론

2.1 등가 무손실 선로를 가진 Chua 회로

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

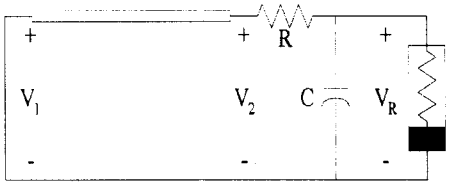

그림 3. 전송 선로를 가진 Chua 회로
Fig. 3. Chua's circuit with a transmission line

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

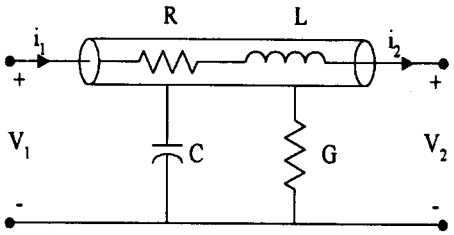

그림4. 전송 선로
Fig.4. A transmission line.

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

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

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.

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

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

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.

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

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

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.

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

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

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

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

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

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.

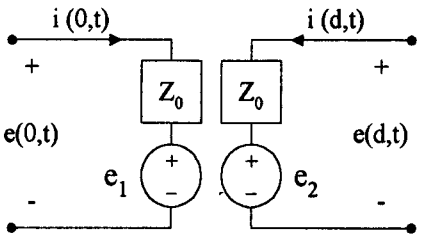

그림 5. 전송 선로의 특성 모델
Fig. 5. The characteristic model of a transmission line

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

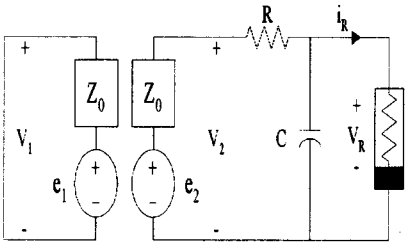

그림 6. 전송 선로를 가진 Chua 회로의 등가회로
Fig. 6. Equivalent circuit of Chua's circuit with a transmission line

2.2 등가 T형 전송선로를 가진 Chus 회로에서의 암호 통신

동일한 Chua 회로 2개를 송신부와 수신부로 놓고 그 사이에 등가 전송 선로를 가진 암호 통신 회로를 그림7에 나타내었다.

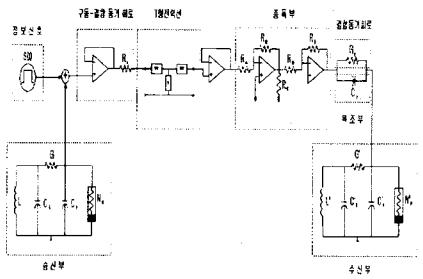

그림7. T형 등가 전송선로를 가진 암호통신 회로
Fig.7 Secure communication circuit with T type equivalent transmission line.

그림7에서 송수신부 및 전송선로부의 상태방정식은 다음과 같다

송신부의 상태 방정식

$$C_1\frac{dv_{c_1}}{dt}=G(v_{c_2}-v_{c_1})-g(v_{c_1})$$

$$C_2\frac{dv_{c_2}}{dt}=G(v_{c_1}-v_{c_2})+i_L \quad (13)$$

$$L\frac{di_L}{dt} = -v_{c_2}$$

등가 전송선로의 상태방정식

$$L_t\frac{di_{L_t}}{dt} = v_{c_1} - (R_t + R_x)i_{L_t} - v_{c_t} + S(t)$$

$$C_t\frac{dv_{c_t}}{dt} = i_{L_t} - (G_0 + G_t)v_{c_t} \qquad (14)$$

수신부의 상태방정식

$$C_1'\frac{dv_{c_1}'}{dt} = G'(v_{c_2}' - v_{c_1}') - g(v_{c_1}') + G_y(v_{c_t} - v_{c_1}')$$

$$C_2'\frac{dv_{c_2}'}{dt} = G'(v_{c_1}' - v_{c_2}') + i_L' \qquad (15)$$

$$L'\frac{di_L'}{dt} = -v_{c_2}'$$

식 (13) ~식 (15)에서 송수신부의 상태 변수 차 관계식을 세우고 안정한 시스템이 되도록 $R_x = 780[\Omega]$, $G_y = 0.005[\mho]$, $C_y = 1[\mu F]$로 정하여 시뮬레이션 하였다.

본 논문에서는 카오스 신호에만 동기하는 회로를 구성하고 결합 저항에 흐르는 송신부와 수신부의 전류차를 검출하는 방법으로 정보 신호를 복조하였다.

정보 신호로는 크기 -400[mV] ~ +400[mV], 주기 5[ms]의 구형파를 인가하여 암호화 통신 상태를 비교하였다. 반송파인 송신부의 v_{c_1} 전압 파형을 그림 7에 나타내었으며

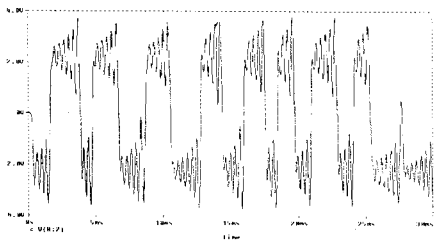

그림 8. 반송파 신호(송신부 신호)
Fig. 8. Carrier signal (transmitter signal)

도청을 가정하여 선로 중간에서 측정한 신호를 그림 9에 나타내었으며 구형파인 정보 신호와 월등히 다른 모양을 보이고 있어서 도청의 의미가 없음을 알 수 있다.

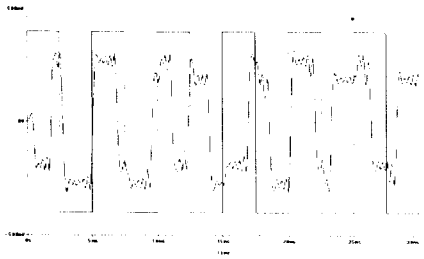

그림 9. 선로 중간에서 도청한 신호
Fig. 9. Wiretapping signal

복조 신호를 3[kHz]의 차단 주파수를 가진 저역 통과 필터를 이용하여 필터링한 결과를 그림 10에 나타내었다.

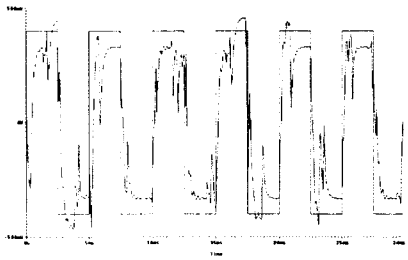

그림 10. 필터링한 후의 복원 신호
Fig. 10. Filtered recovery signal

필터링 결과 구형파 형태로 어느 정도 복원 할 수 있었으나 등가 T형 선로의 L, C에 의한 동기화의 영향 때문에 복조 성능이 우수하지 않음을 알 수 있다

3. 결 론

등가 전송 선로를 이용한 카오스 암호 통신은 전송선로의 L, C에 의한 시간 지연이 있는 동기화 때문에 수신단에서 완전한 정보 신호를 복원할 수 없었으나 신호의 크기와 주파수 제한을 둔 디지털 정보 신호의 암호화 통신에 충분히 적용할 수 있음을 제시하였다.

[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] F.H. Branin,JR. "Transient Alalysis of Lossless Tranmission Lines", Proc. IEEE. vol.55 pp. 2112-2113. 1967.

[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
1995.

[7] 배영철,손영우,고윤석, " 무손실 시간 지연을 갖는 Chua 회로에서의 카오스 해석", 한국통신학회논문지, 22권 2호 pp. 418 - 324, 1997.

[8] 배영철,고재호,유창완,홍대승,임화영, " 손실 전송선로를 가진 Chua 회로에서의 카오스 비밀 통신에 관한 연구", 한국통신학회논문지, 24권 10A pp. 1539 - 1545, 1999.

[9] 배영철,고재호,유창완,홍대승,임화영, " RLCG 전송선로를 가진 Chua 회로에서의 카오스 동기화에 관한 연구", 한국통신학회논문지, 24권 11B pp. 2030 - 2035, 1999.