전력선을 이용한 Chua 회로에서의 카오스 비밀통신

Chaos Secure Communication of Power Line Chua's Circuit

배 영 철, 김 이 곤
여수대학교 전기공학과

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 circuitsare proposed and a transmission 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 power lime.

I. 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.

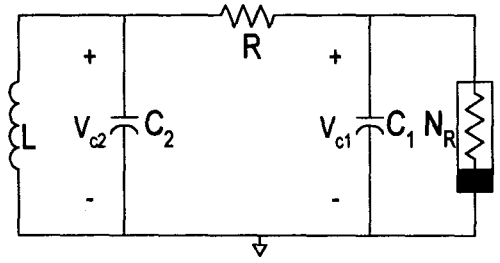

그림 1. Chua 회로

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

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

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

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

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.

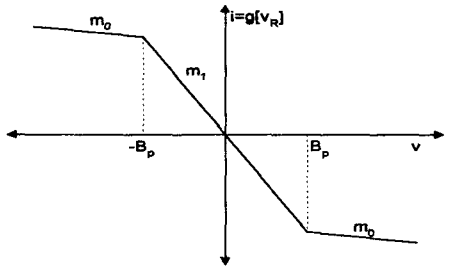

그림2. 비선형 저항의 전압 전류 특성

본 논문에서는 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 검토하고 파라미터 부정합에 의한 안전성을 평가하였다.

Ⅱ. 관계이론

2.1 등가 전송선로를 가진 Chua 회로

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

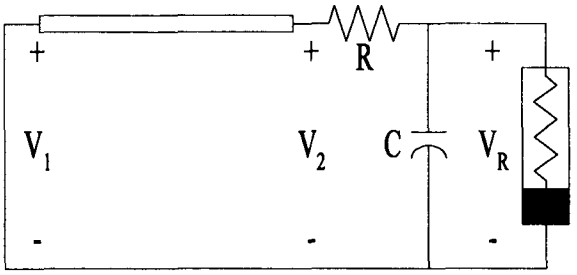

그림 3. 전송 선로를 가진 Chua 회로

Branin[7]는 무손실 전송선로의 과도 해석을 위한 특성곡선법을 제안하였다.그림4와 같은 전송 선로의 특성 방정식은 다음과 같이 표시된다.

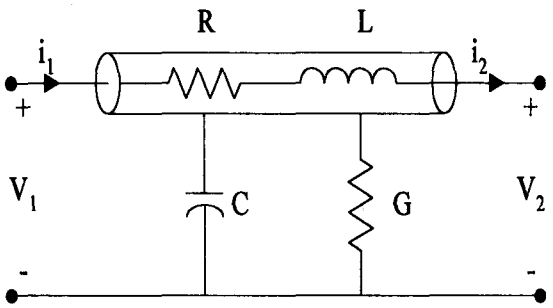

그림4. 전송 선로

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

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

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.

식(3)와 식(4)은 입사파와 반사파 전압원을 이용하여 다음과 같은 수식으로 정리 할 수 있다

$$e(d,t)=-Z_0 i(d,t)-e_2(0,t-\tau) \qquad (5)$$

$$e(0,t)=+Z_0 i(0,t)-e_1(d,t-\tau) \qquad (6)$$

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(5)과 식(6)의 등가 회로를 그림 5에 나타내었다.

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

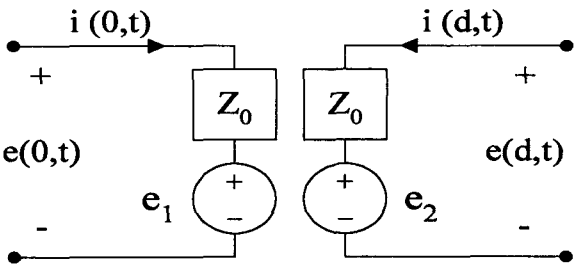

그림 5. 전송 선로의 특성 모델

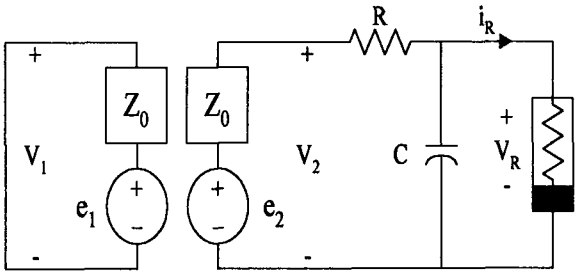

그림 6. 전송 선로를 가진 Chua 회로의 등가회로

2.2 전력선을 가진 Chua 회로에서의 카오스 암호 통신

동일한 Chua 회로 2개를 송신부와 수신부로 놓고 그 사이에 T형rhk π형 전력선을 가진 비밀 통신 회로를 그림7, 8에 나타내었다.

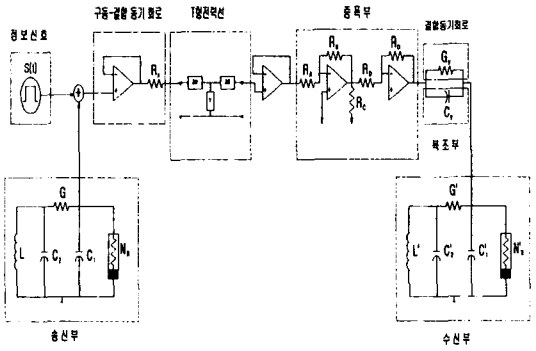

그림7. T형 전력선을 가진 비밀통신 회로

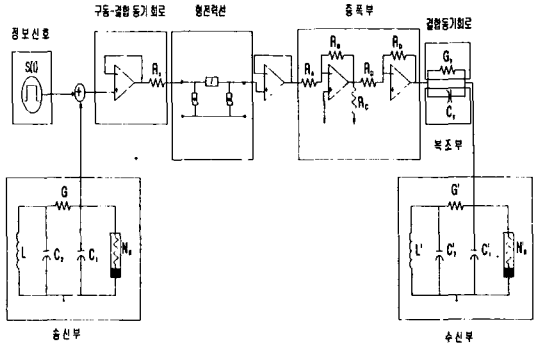

그림8. π형 전력선을 가진 비밀통신 회로

그림7,8에서 송수신부 및 전송선로부의 상태방정식은 다음과 같다

송신부의 상태 방정식

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

손실 전송선로의 상태방정식

$$L_t\frac{di_{L_t}}{dt}=v_{c_1}-(R_t+R_x)i_{L_t}-v_{c_t}+S(t)$$
$$C_t\frac{dv_{c_t}}{dt}=i_{L_t}-G_0v_{c_t} \qquad (8)$$

수신부의 상태방정식

$$C_1'\frac{dv_{c_1}'}{dt}=G'(v_{c_2}'-v_{c_1}')-g(v_{c_1}')+G_y(v_{c_t}-v_{c_1}')$$
$$C_2'\frac{dv_{c_2}'}{dt}=G'(v_{c_1}'-v_{c_2}')+i_L' \qquad (9)$$
$$L'\frac{di_L'}{dt}=-v_{c_2}'$$

식 (7) ~식 (9)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 9에 나타내었으며 수신부에서 동기화된 v_{c_1}'의 전압 파형을 그림 10에 나타내었다.

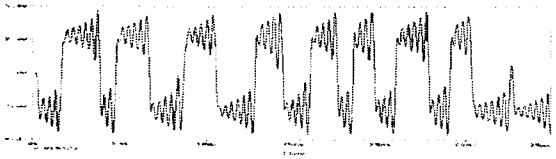

그림 9. 반송파 신호(송신부 신호)

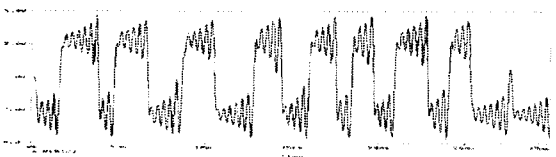

그림 10. 수신부의 카오스 신호

그림 9와 10에서 송신 신호와 수신 신호가 같은 형태를 이루고 있어서 동기화 현상이 이루어짐을 알 수 있다.

도청을 가정하여 선로 중간에서 측정한 신호를 그림 11에 나타내었으며 구형파인 정보 신호와 월등히 다른 모양을 보이고 있어서 도청의 의미가 없음을 알 수 있다.

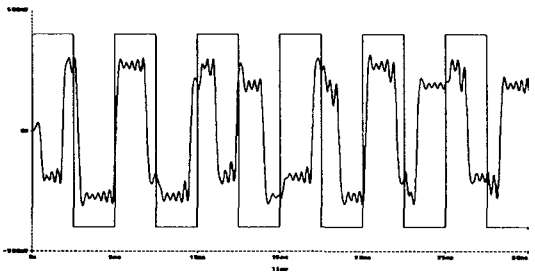

그림 11. 선로 중간에서 도청한 신호

복조 신호를 3[kHz]의 차단 주파수를 가진 저역 통과 필터를 이용하여 필터링한 결과를 그림 12에 나타내었다.

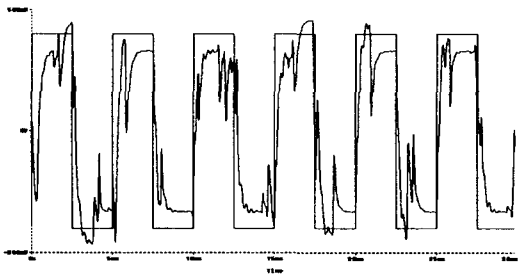

그림 12. 필터링한 후의 복원 신호

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

Ⅲ.카오스 비밀 통신에서의 안전성 검토

카오스 회로는 초기치에 민감한 조건 때문에 동일한 2개의 카오스 회로에서 동기화를 이루는 것이 어려운 것으로 알려져 있다.

Chua 회로에서는 파라미터 값이 C_1, C_2, L, G, m_0, m_1을 가지며 두개의 동일한 회로를 구성하여 비밀 통신에 이용하고자 할 때는 이들 파라미터 값이 모두 일치해야만 동기화를 이룰 수 있다. 만약 이들 파라미터 값 중 하나라도 미소하게라도 불일치 한다면 동기화를 이룰 수 없으며 아울러 비밀 통신도 불가능하다.

본 연구에서는 이 파라미터 값을 키 신호로 이용

하여 6개의 파라미터 값이 미소하게 불일치 한 경우의 비밀 통신 결과를 나타내었다.

그림 13은 C_1 파라미터 값이 송신부에서 10nF, 수신부에서 9.9nF의 미소하게 불일치 한 경우의 복원 결과를 나타내었다.

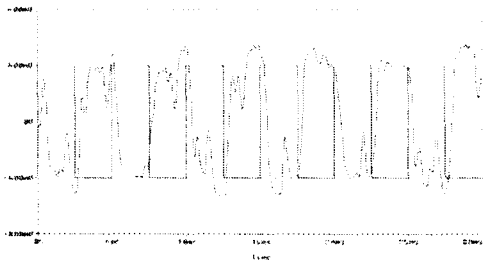

그림 13. 파라미터 송신측 $C_1 = 10nF$
수신측 $C_1 = 9.9nF$ 일 때의 복원 결과

그림 13에서 보듯이 키 값이 약간 불일치 하는 경우에 그림 12과의 결과와 다르게 나타남을 알 수 있다. 이 결과 선로 중간에서 송수신기와 동일한 Chua 회로를 이용하여 공격한다 할지라도 6개의 파라미터 값을 송수신부의 키값에 의해 랜덤하게 변경한다면 도청은 불가능하며 공격자에 대한 안전성 즉 키를 모르고 공격하는 경우의 안전성을 확보할 수 있다. 실제 다른 파라미터보다 비선형 저항의 기울기인 m_0, m_1은 아주 미소하게 변하여도 큰 효과를 낼 수 있다.

Ⅳ. 결 론

본 논문에서는 전력선을 가진 Chua 회로에서의 카오스 비밀 통신 방법에 대하여 연구하였다. 두 개의 동일한 Chua 회로에 T형 및 π형 전력선을 두어 전송로를 구성한 후 송신부와 전력선 사이는 구동-결합 동기 이론을 전력선과 수신부 사이는 결합 동기 이론을 적용한 동기화 방법을 제시하였으며, 송신부에서 가산기를 이용하여 정보 신호와 카오스 신호를 합성하고 수신부에서 이들 신호를 분리하는 비밀 통신을 행하고 그 안정성을 평가하였다. 앞으로 디지털 방식에 의한 동기화와 실제 전송로의 적용에 대한 비밀 통신의 질적인 향상이 과제로 남는다.

이 논문은 과학기술부, 과학재단 지정 지역협력 센터인 여수대학교 설비자동화 및 정보 시스템 연구개발센터의 연구비 지원에 의해 연구되었음.

Ⅴ. 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.