등가 유무선 선로를 가진 Chua 회로에서의 카오스 비밀통신

Chaos secure communication of Chua's circuit with equivalent wire and wireless transmission

배 영 철
여수대학교 전기공학과
Young-chul Bae
Nat'l Yosu University
E-mail : ycbae@yosu.ac.kr

Abstract

In this paper, we formed a transmitter and receiver by using three identical Chua's circuits and then formed wire and wireless transmission line from the channel which was between those three circuits. We proposed a secure communication method in which the desired information signal was synthesized with the chaos signal created in a Chua's circuit and sent to the transmitter through channel. Then the signal was demodulated receiver of Chua's circuit. The method we used to accomplish the secure communication was synthesizing the desired information with the chaos circuit by parallel connection in a wireless transmission line. After transmitting the synthesized signal to the wire and wireless transmission line, we confirmed the actuality of the secure communication by separating the information signal and the chaos signal in the receiver.

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 발진 회로다.

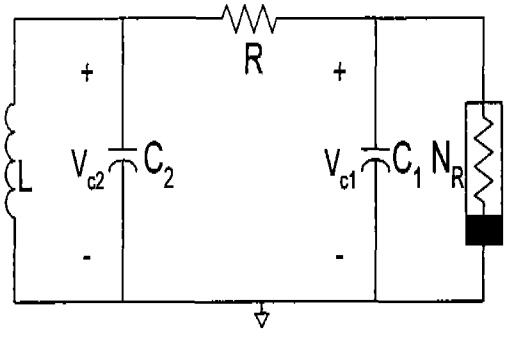

그림 1. Chua 회로

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.

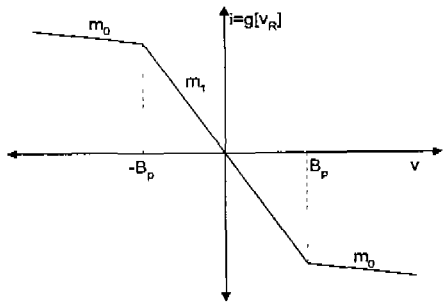

그림2. 비선형 저항의 전압 전류 특성

본 논문에서는 카오스 동기화 및 암호화 통신을 위해 동일한 3개의 Chua 회로로 유무선의 송신부와 수신부로 각각 구성하고 이 3 회로 사이에 등가 무선선로와 유선선로를 구성하였다. Chua 회로에서 발생한 카오스 신호를 반송파로 정하고 전송하고자 하는 정보 신호를 카오스 신호인 반송파에 합성하여 무선 채널과 유선 채널을 통해 수신부에 전송하여 수신부에서 카오스 신호인 반송파와 정보 신호를 분리하는 복조 방법으로 실제 선로서 적용 가능한 암호화 통신 방법을 제시하였다.

2. 유무선 전송선로를 가진 Chua 회로에서의 카오스 비밀통신

카오스 암호화 통신은 불규칙한 카오스 신호를 반송파로 반송파에 정보 신호를 합성하여 통신을 행하므로 높은 보안성을 유지할 수 있어 앞으로 그 필요성이 증대되고 있다.

카오스 암호화 통신은 송신부에서 잡음과 같은 불규칙한 카오스 신호에 정보 신호를 합성하여 수신부에서 카오스 신호와 정보 신호를 분리하는 통신 방법이다. 카오스 암호화 통신은 정보 신호가 카오스 신호보다 월등히 크지 않으면 카오스 암호화 통신을 위해 합성된 신호는 카오스 성질을 가질 뿐 아니라 송신부에서 반송파로 이용하는 신호 속에 숨겨지기 때문에 중간에 도청을 한다 할지라도 정보 신호가 검출되는 것이 아니고 카오스 신호가 검출되므로 안전한 암호화 통신을 할 수 있다.

카오스 암호화 통신은 이러한 특성을 이용하여 카오스 신호에 정보 신호를 합성하는 방법이 제시되었으나 이는 정보 신호가 카오스 신호에 비해 충분히 작아야하고 정보 신호를 단일 주파수인 정현파를 가해 암호 통신 적용 사례로 적절치 못하였으며 선로에 대한 정확한 제시가 없었다.

본 논문에서는 암호화 통신을 위해 불규칙한 카오스 신호를 반송파로 정하고 전송로를 유무선 선로로 구성하였으며 카오스 회로와 병렬로 정보 신호를 합성하는 방법을 제시하였다.

합성된 신호를 전송 선로를 통해 전송하였으며 수신부에서 정보 신호와 카오스 신호를 분리하는 복조 방법은 송신부에서 정보 신호를 분류하는 방법을 적용하였으며 이를 Pspice로 시뮬레이션 하였다.

또한 암호 통신중 선로 중간에서 도청한다는 가정 하에 도청된 신호와 복원된 신호를 비교하여 암호화 통신이 이루어졌음을 확인하였다.

두 개의 동일한 Chua 회로에서 파라미터 값의 일치하지 않을 때와 일치할 때의 암호화 결과를 비교하여 실제 선로에서의 적용 가능성을 알아보았다.

제안된 암호화 통신 방법은 지금까지 연구된 방법보다 정보 신호의 크기를 크게 하여도 동기화를 이루었으며 우수한 복원 능력을 가졌음을 확인하였으며 실선로에서도 이용할 수 있도록 하였다.

카오스 암호화 통신 회로를 그림 3에 나타내었다.

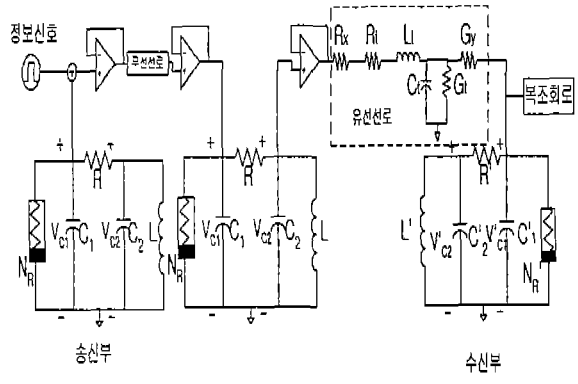

그림 3. 유무선 선로를 가진 카오스 비밀 통신 회로

그림 3의 상태방정식을 세우면 다음과 같다.

무선선로의 송신부의 상태방정식

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

$$C_2\frac{dv_{C_2}}{dt} = G(v_{C_1} - v_{C_2}) + i_L \qquad (3)$$

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

무선선로의 수신부 상태 방정식

$$C_2\frac{dv_{c_2}}{dt} = G(v_{c_1} - v_{c_2}) + i_L$$
$$L\frac{di_L}{dt} = -v_{c_2} \quad (4)$$

유선선로의 송신부 상태방정식

$$C_1\frac{dv_{c_1}}{dt} = G(v_{c_2} - v_{c_1}) - g(v_{c_1})$$
$$C_2\frac{dv_{c_2}}{dt} = G(v_{c_1} - v_{c_2}) + i_L \quad (5)$$
$$L\frac{di_L}{dt} = -v_{c_2}$$

유선선로 전송선로 상태 방정식

$$L_t\frac{di_{L_t}}{dt} = v_{c_1} - (R_x + R_t)i_{L_t} - v_{c_t}$$
$$C_t\frac{dv_{c_t}}{dt} = i_{L_t} - (G_t + G_y)v_{c_t} + G_y v_{c_1}' \quad (6)$$

유선선로 수신부의 상태방정식

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

식 (3) ~식 (7)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 4에 나타내었으며 수신부에서 동기화된 v_{c_1}'의 전압 파형을 그림 4에 나타내었다.

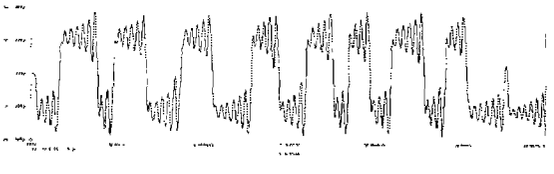

그림 4. 반송파 신호(송신부 신호)

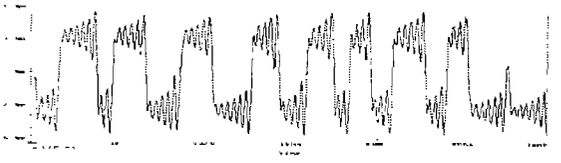

그림 5. 수신부의 카오스 신호

그림 4와 5에서 송신 신호와 수신 신호가 같은 형태를 이루고 있어서 동기화 현상이 이루어짐을 알 수 있다.

복조 신호를 3[kHz]의 차단 주파수를 가진 저역 통과 필터를 이용하여 필터링한 결과를 그림 6에 나타내었다.

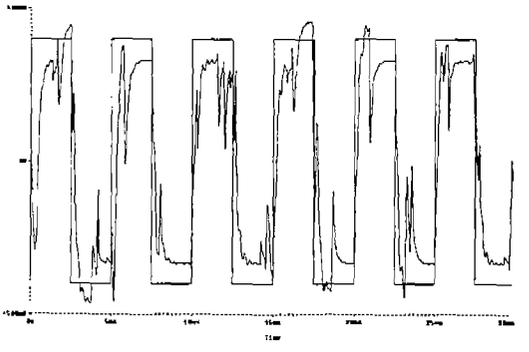

그림 6. 필터링한 후의 복원 신호

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

3. 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 이용하여개의 파라미터 값이 미소하게 불일치 한 경우의 비밀 통신 결과를 나타내었다.

그림 7은 C_1 파라미터 값이 송신부에서 10nF, 수신부에서 9.9nF의 미소하게 불일치 한 경우

의 복원 결과를 나타내었다.

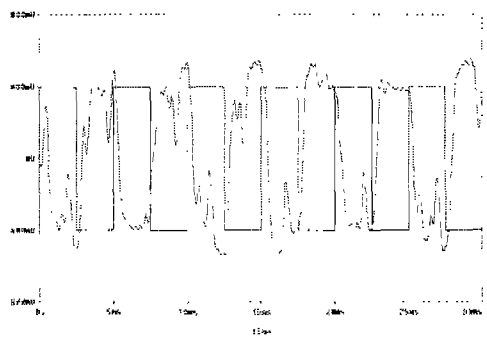

그림 7. 파라미터 송신측 $C_1 = 10nF$,
수신측 $C_1 = 9.9nF$ 일 때의 복원 결과

그림 7에서 보듯이 키 값이 약간 불일치 하는 경우에 그림 6과의 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_1 은 아주 미소하게 변하여도 큰 효과를 낼 수 있다.

4. 결 론

본 논문에서는 유무선 선로를 가진 Chua 회로에서의 카오스 비밀 통신 방법에 대하여 연구하였다. 3 개의 동일한 Chua 회로에 등가 무선 및 유선 회로를 두어 전송로를 구성한 후 무선부에서는 구동동기 이론을 유선부에서는 구동-결합 및 결합동기 이론을 적용하는 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.

감사의 글

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

[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] 배영철,고재호,임화영,유창완,홍대승, "손실전송선로를 가진 Chua 회로에서의 카오스 비밀 통신에 관한 연구", 한국통신학회논문지, 24권, 10A호, 1539-1545. 1999.

[8] 배영철,임화영, "RLCG 전송선로를 가진 Chua 회로에서의 카오스 동기화에 관한 연구", 한국 통신학회논문지, 24권 11B호, 2030-2035. 1999.

[9] 배영철, " 등가전송선로를 가진 Chua 회로에서의 카오스 동기화 및 암호화 통신에 관한 연구", 한국 해양정보통신학회논문지, 4권, 1호, 241-250. 2000.

[10]배영철,고재호,유창완,홍대승,임화영, "리아프노프 함수를 이용한 Chua 오실레이터 회로에서의 카오스 제어", 한국해양정보통신학회논문지, 3권, 1호, 113-120. 1999.