Chua 회로에서의 카오스 비밀통신

배 영 철

여수대학교 전기공학과

Chaos Secure Communication using Chua Circuit

Young-chul Bae

Nat'l Yosu University

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

Abstract

In this paper, we formed a transmitter and receiver by using two identical Chua's circuits and then formed wireless transmission line from the channel which was between those two 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 wireless transmission line, we confirmed the actuality of the secure communication by separating the information signal and the chaos signal in the receiver. In order to confirm the security, we compared the wiretapped signal and the recovery signal under the assumption that the wiretapping had taken place.

In order to separate the two signals, we transformed the information signal to a current source in the transmitter and detected the current 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 발진회로다.

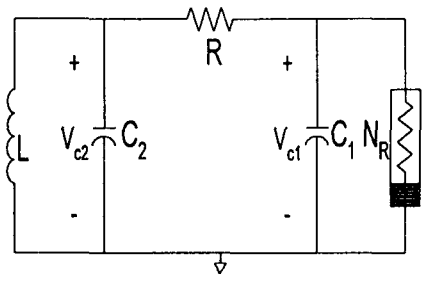


그림 1. Chua 회로

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

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

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

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

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

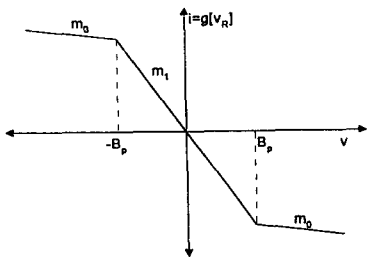


그림2. 비선형 저항의 전압 전류 특성

본 논문에서는 카오스 동기화 및 암호화 통신을 위해 동일한 2개의 Chua 회로로 송신부와 수신부로 각각 구성하고 이 두 회로 사이에 무선 전송로를 구성하였다. Chua 회로에서 발생한 카오스 신호를 반송파로 정하고 전송하고자 하는 정보 신호를 카오스 신호인 반송파에 합성하여 무선 채널 통해 수신부에 전송하여 수신부에서 카오스 신호인 반송파와 정보 신호를 분리하는 복조 방법으로 실제 선로에서 적용 가능한 암호화 통신 방법을 제시하였다.

2. Chua 회로에서의 카오스 암호화 통신

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 작아야 하고 정보 신호를 단일 주파수인 정현파를 가해 암호통신 적용 사례로 적절치 못하였으며 선로에 대한 정확한 제시가 없었다.

본 논문에서는 암호화 통신을 위해 불규칙한 카오스 신호를 반송파로 정하고 전송로를 무선 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 전류원으로 변환한 후 수신부에 전류를 검출하는 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 정보 신호를 단일 주파수 성분의 정현파가 아닌 음성 신호에 가까운 다중 주파수 성분의 구형파를 적용하여 실제 선로에서도 이용할 수 있도록 하였다.

카오스 암호화 통신 회로를 그림 3에 나타내었다.

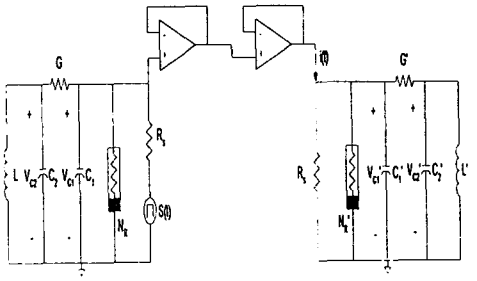


그림 3. 카오스 비밀 통신 회로

수신부에서 정보 신호가 보다 큰 S/N비를 갖도록 하기 위해 정보 신호를 카오스 신호에 병렬로 접속하여 전류원의 역할을 하게 하고 수신부에서는 이 전류값을 구하면 이 전류값이 바로 정보 신호가 된다.

그림 3의 상태방정식을 세우면 다음과 같다.

송신부의 상태방정식

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

$$C_2\frac{dv_{c_2}}{dt}=G(v_{c_1}-v_{c_2})+i_L \qquad (2\text{-}1)$$

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

수신부의 상태방정식

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

$$C_2'\frac{dv_{c_2}'}{dt}=G'(v_{c_1}'-v_{c_2}')+i_L' \qquad (2\text{-}2)$$

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

여기서 동기화 결과로 $v_{c_1}(t)=v_{c_1}'(t)$이다.

식 (2-2)의 첫 번째 수식으로부터 정보 신호 $e(t)$를 구하면 다음과 같다.

$$e(t)=R_s[\,C_1\frac{dv_{c_1}}{dt}-G(v_{c_2}-v_{c_1})+g(v_{c_1})+\frac{v_{c_1}}{R_s}\,] \qquad (2\text{-}3)$$

식 (2-2)의 첫 번째 수식으로부터 수식으로 구하면 다

음과 같다.

$$i(t)=[C_1'\frac{dv_{c_1}'}{dt}-G'(v_{c_2}'-v_{c_1}')+g(v_{c_1}')+\frac{v_{c_1}'}{R_s}] \quad (2\text{-}4)$$

식 (2-4)는 식 (2-3)의 우변항에서 [ ]안에 있는 수식과 같으므로 수식으로 식 (2-3)로부터 다음과 같이 구할 수 있다.

$$i(t)=\frac{e(t)}{R_s} \quad (2\text{-}5)$$

식 (2-5)로부터 전류는 정보 신호에 비례함을 알 수 있다. 정보 신호는 그림 4와 같은 전류 검출기(Current detector)를 이용하여 복원하였다.

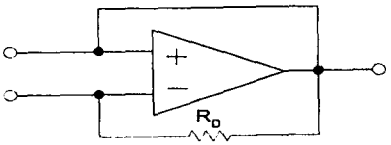
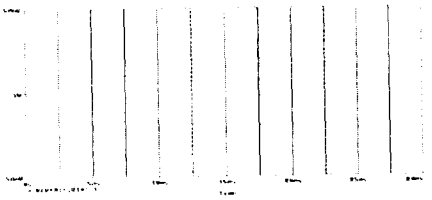


그림4. 전류 검출기

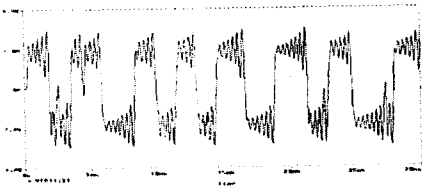
본 논문에서는 전류 검출기의 저항 R_D와 구동-결합에 의한 저항 R_x와의 값을 직렬로 고려하여 $2.8K\Omega$으로 $R_s=33K\Omega$으로 정하여 컴퓨터 시뮬레이션을 다음과 같이 행하였다.

3. 완전 동기화에 의한 카오스 암호화 통신

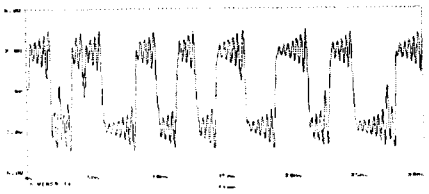
그림 3의 무선 통신에 의한 완전 동기화에 의한 카오스 암호화 통신의 결과를 그림 5에 나타내었다. 정보 신호를 -50mA～+50mA의 크기를 가진 다중 주파수의 구형파를 이용하였다.



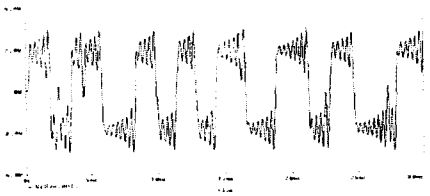
(a) Information signal of rectangular wave



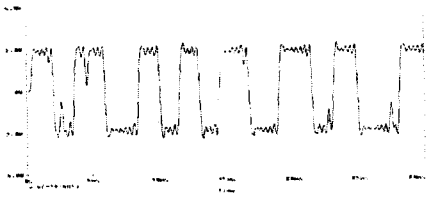
(b) Carrier signal (Chaotic signal)



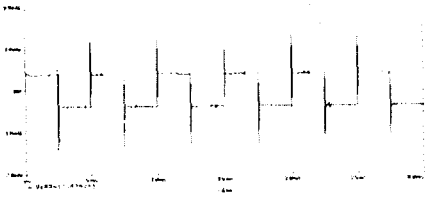
(c) Mixed signal with information signal and chaotic signal



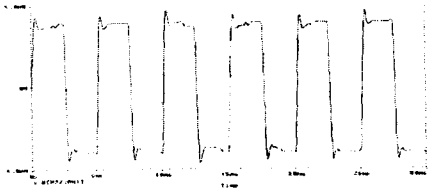
(d) Wiretapping signal before recovery



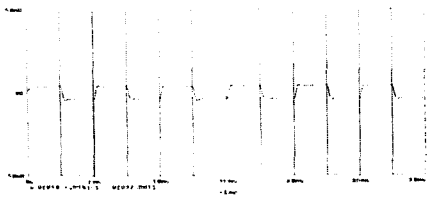
(e) Filtering signal of wiretapping signal



(f) Recovery signal



(g) Filtered recovery signal



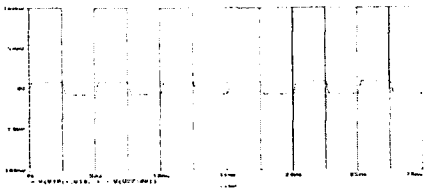
(h) Compare of information signal and recovery signal

그림 5. 비밀통신 결과

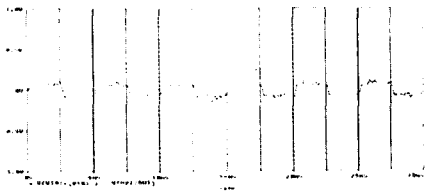
그림 5에서 확인할 수 있듯이 무선 선로에서는 송신부의 신호와 수신부의 신호가 동기화 되었음을 확인할 수 있으며 중간에서 도청을 하였을 때의 신호는 카오스 신호가 되며 필터링을 하여도 정보 신호를 복원할 수 없었다.
전류 검출기에 의해 복원된 신호는 정보 신호와 비교하여 거의 일치된 신호를 얻을 수 있어 안전한 암호화 통신이 됨을 확인할 수 있었다.

4.정보신호 크기를 변화하였을 때의 암호화 통신

정보 신호의 크기는 카오스 신호에 충분히 숨길 수 있고 동기화를 유지하는 범위 내에서 작은 신호를 주어야 하는 것으로 알려져 있다.
Chua가 제시한 논문에서는 정보 신호의 크기가 10mV의 이상이 되면 동기화가 깨지고 정보 신호 복원이 잘 되지 않는 문제점이 있다. 본 논문에서 제안한 방법은 Chua가 제안한 방법보다 더 큰 정보 신호를 보낼 수 있어 큰 S/N비를 갖는다. 그림 6에 정보 신호 크기를 변화했을 때의 암호화 통신 결과를 나타내었다.



(a) When information signal magnitude 100mV



(b) When information signal magnitude 1V

그림6. 정보 신호 크기 변화에 따른 비밀통신

그림 6에서 확인 할 수 있듯이 정보 신호 처리가 100[mV]에서는 완전한 복원 상태를, 1[V]에서는 복원력이 떨어지는 것으로 나타났으며 Chua가 제시한 방법보다 더 큰 S/N비를 가짐을 확인할 수 있다.

5. 결 론

본 논문에서는 무선 전송선로를 가진 Chua 회로에서의 및 카오스 암호화 통신에 대하여 실제 적용 가능성을 살펴보았다.
무선 전송선로 암호화 통신을 위해서 Chua 회로와 병렬로 정보 신호를 합성하여 전류원으로 구성한 후 수신부에서 전류를 검출하는 전류 검출기(current detector)를 설계하여 정보 신호와 카오스 신호를 분리하였으며 분리된 신호를 필터링하여 정보 신호와 근접한 신호를 복원하였다.
선로 중간에서 정보 신호를 도청한다는 가정하에 도청하였을 때의 신호와 복원 신호 및 정보 신호를 비교하여 도청 신호에서 정보 신호를 추출 할 수 없어 완전한 암호화 통신이 됨을 확인하였다.

이 논문은 과학기술부, 과학재단 지정 지역협력 센터인 여수대학교 설비자동화 및 정보 시스템 연구개발 센터의 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