전송선로를 가진 Chua 회로에서의 카오스 암호화

*고재호, **배영철, *임화영
* 광운대학교 제어계측공학과, ** 산업 기술 정보원

Chaos Secure Communication of Chua's Circuit with Transmission Line

*Ko Jae-Ho, **Bae Young-Chul, *Yim Wha-Young
* Dept. of Control and Instrumentation Eng, Kwang Woon Univ., ** KINITI

Abstract

In this paper, a transmitter and a receiver using two identical Chua's circuits are proposed and a 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.

After transmitting the synthesized signal through the wire transmission system, it is confirmed the feasibility of the secure communication from result of demodulated signals and recovered wire tapped signals.

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.

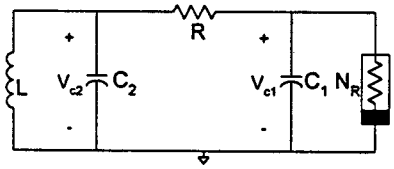

그림 1. Chua 회로
Fig. 1. Chua's circuit

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.

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

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

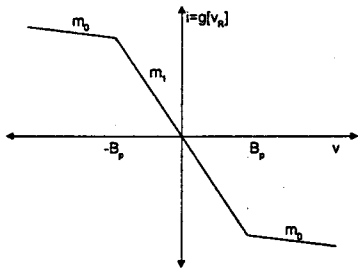

그림2. 비선형 저항의 전압 전류 특성
Fig.2. v-i characteristic of nonliner resistor

본 논문에서는 유선 선로를 대상으로 가산기를 이용하여 정보 신호와 카오스 신호를 합성하였으며 무선선로에서는 카오스 회로와 병렬로 정보 신호를

합성하는 방법을 시도하였다. 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 검토 하였다. 송신부와 수신부에 있는 각각의 Chua 회로에서 각 파라미터 값이 일치 할 때와 일치하지 않을 때의 동기화 특성의 영향에 따른 암호화 결과를 비교하였다.

본 연구에서는 동일한 2개의 Chua 회로 사이에 전송선로를 둔 카오스 동기호에 관하여 연구하였다

2. 전송선로를 가진 카오스 암호화 통신

분포정수를 가진 유선 선로의 통신에서의 카오스 암호화 통신 회로를 그림 3에 나타내었다. 송신부에서 카오스 신호와 정보 신호의 합성은 가산기를 이용하였으며 선로 중간에 신호 도청을 가정하고 이로 인한 수신 신호의 크기를 보상하기 위한 증폭 회로로 구성하였다. 송신부와 RLCG 전송선로는 구동-결합 동기 방법을, RLCG 전송선로와 수신부는 결합 동기 방법을 써서 동기화를 이루었으며 수신부에서 결합 저항과 병렬로 콘덴서를 연결하여 불필요 신호를 제거하는 회로를 구성하였다.

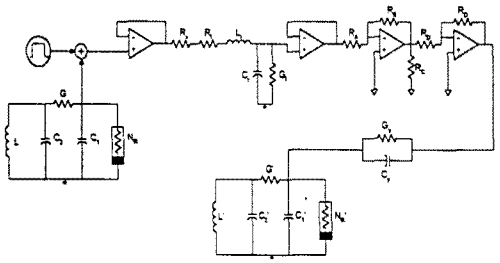

그림 3. 유선 선로의 카오스 암호화 통신 회로
Fig. 3. Chaos secure communication circuit with wire transmission line

그림 3 회로의 상태 방정식은 다음과 같다.

송신부의 상태 방정식

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

$$C_2\frac{dv_{c_2}}{dt}=G(v_{c_1}-v_{c_2})+i_L \qquad (3)$$

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

RLCG 전송선로의 상태방정식

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

$$C_t\frac{dv_{c_t}}{dt}=i_{L_t}-(G_0+G_t)v_{c_t} \qquad (4)$$

증폭부 및 결합 저항부의 상태방정식

$$C_y\frac{dv_{c_y}}{dt}=-\frac{R_B}{R_AR_D}v_{c_t}-G_yv_{c_y}$$

$$C_1\frac{dv_{c_1}'}{dt}=G(v_{c_2}'-v_{c_1}')-g(v_{c_1}')-\frac{R_B}{R_AR_D}v_{c_t} \qquad (5)$$

수신부의 상태방정식

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

$$C_2'\frac{dv_{c_2}'}{dt}=G'(v_{c_1}'-v_{c_2}')+i_L' \qquad (6)$$

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

식 (3) ~식 (6)에서 송수신부의 상태변수 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

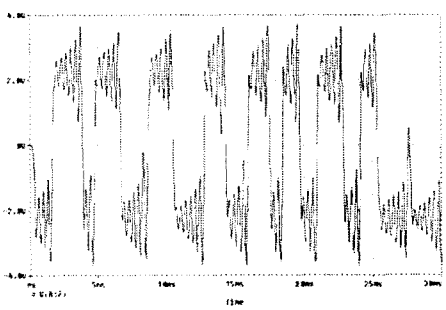

그림 4. 반송파 신호(송신부 신호)
Fig. 4. Carrier signal (transmitter signal)

수신부에서 동기화된 v_{c_1}'의 전압 파형을 그림 5에 나타내었다.

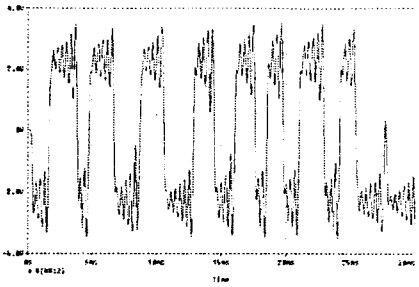

그림 5. 수신부의 카오스 신호
Fig. 5. Chaos signal of receiver signal

그림 4와 5에서 송신 신호와 수신 신호가 같은 형태를 이루고 있어서 동기화 현상이 이루어짐을 알 수 있다.
송수신 신호 v_{c_1}과 v_{c_1}'를 그림 6에 비교해 보였다. 두 신호의 동기화기 이루어졌으나 전송선로의 L, C 영향으로 시간지연(위상차)가 나타난다.

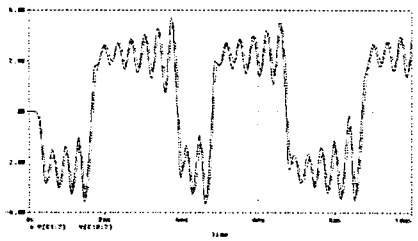

그림 6. 송신부와 수신부의 시계열 데이터 비교
Fig 6. Comparing of time series of transmitter-receiver

도청을 가정하여 선로 중간에서 측정한 신호를 그림 7에 나타내었으며 구형파인 정보 신호와 월등히 다른 모양을 보이고 있어서 도청의 의미가 없음을 알 수 있다.

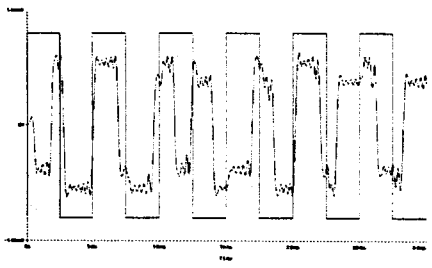

그림 7. 선로 중간에서 도청한 신호
Fig.7. Wiretapping signal

복조 신호를 3[kHz]의 차단 주파수를 가진 저역통과 필터를 이용하여 필터링한 결과를 그림 8에 나타내었다. 필터링 결과 구형파 형태로 어느 정도 복원 할 수 있었으나 전송선로의 L, C에 의한 동기화의 영향 때문에 복조 성능이 우수하지 않음을 알 수 있다.

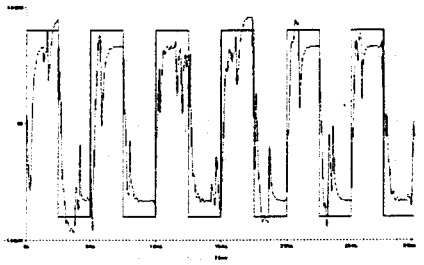

그림 8. 필터링한 후의 복원 신호
Fig.8. Filtered recovery signal

지금까지 Chua 회로의 동기화에 관한 연구는 결합 동기와 구동 동기 이론은 결합 저항과 버퍼를 사용하여 송수신부를 결합하거나 구동시키고 있어서 실제 선로를 고려하지 않은 경우의 동기화를 다룬 것이다.

3. 결 론

RLCG 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 정보신호의 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] 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.