Small World 구축을 위한 비밀 통신 기법

배영철*, 구영덕

*여수대학교 전자통신기공학부,한국과학기술정보연구원

The Secure Communication Method for Build Small World

Young-Chul Bae, Young-Duk Koo

*Nat'l Yosu University, KISTI

E-mail : ycbae@yosu.ac.kr

Abstract

In this paper, we proposed that the secure communication method for build small world. In order to secure communication in the small world, we used Chua's oscillator which well represent the chaos dynamics and composed several stage with Chua's oscillator by using coupled synchronization method. This paper shows a secure communication result in the small world network using coupled synchronizaton method.

1. 서 론

네트워크들은 현재 우리 마음속에 깊숙이 자리 잡고 있다. 때때로 우리는 네트워크의 힘을 두려워 한다. 1996년 8월 10일 미국 오레곤주에서 발생한 2개의 전력선 사고로 인하여 11개 주와 2개의 캐나다 지방의 약 16시간 동안 700만의 주민이 전기를 사용하지 못하는 고통을 경험하였다. 또한 최근의 일로서 2003년 8월 14일 미국 북동부 지역에서 발생한 최악의 정전으로 인하여 미국 북동부 지역과 캐나다 지역에 오랫동안 정전이 되어 800만 주민이 전기 없는 고통 속에 보내야만 했다. 2000년 5월 4일 Love Bug worm 바이러스가 인터넷을 공격하여 전세계에 걸쳐 수십 억 $의 손해를 입혔다.

과학자들은 네트워크를 오래 동안 생각해 왔었다. 과학자들은 주로 식료품 웹상의 위상[1-2], 전력 계통 그리드, 셀룰러와 메타볼릭 네트워크[3-6], WWW(World Wide Web)[7], 인터넷 백본[8], 과학자 공동 저자와 인용 네트워크[9], 전화 호출 그래프[10], 등에 관심을 가지고 연구해 왔다.

전세계 어느 곳이든 구석진 곳에서 일어나는 일도 실시간으로 쉽게 알 수 있는 세상이 우리 눈앞에 다가와 있다. 이러한 현상은 통신과 네트워크의 발달에 크게 힘을 입고 있다고 해야할 것이다. 지구촌을 하나로 묶고자 하는 현상을 우리는 small world 또는 scale free라고 부른다.

Small world 또는 scale free를 위한 통신 시스템이 거대화, 복잡화되어 감에 따라 여러 가지 해결해야하는 문제를 가지고 있다. 그것은 바로 네트워크의 동기화와 비동기화에 대한 문제이다.

small world 또는 scale free에 대한 연구로는 Stenen H. Strogatz가 제시한 small world에 대한 동적 특성을 연구[11]한 경우가 있으며 이는 통계물리와 비선형 동력학을 이용하여 통계적이며 경험적인 방법을 통하여 네트워크를 분석하는 기법을 제공하였다. 또한 L.A.N Amaral 등은 small network 종류에 대한 다양한 분류 기법을 제시[12]한 연구도 있었다. Debra. S. Goldberg 등은 small network에서 실험적으로 유도된 상호 작용에 대한 접속 가능성을 확인한 연구[13]도 있다. 기존의 small world에 대한 모든 연구들은 small world를 왜 구성해야만 하는지에 대한 이유와 그 구성 방법 및 종류에 대하여 언급하였을 뿐 실제적으로 small world를 구축하기에 필요한 동기화 기법 문제를 완전하게 제시한 해법은 없으며 이에 대한 관련 연구가 필요한 실정이다.

이에 본 연구에서는 small world 구축을 위한 비밀통신 기법을 제시하고 그 결과를 검증하였다.

2. Small World

2.1. Small World 네트워크

Small world 구축을 위한 네트워크 구성을 위해서는 그림 1 중간 형태와 같은 정규적이지도 않고 랜덤하지도 않는 네트워크를 구성하여야 한다. 네트워크 구성에 대한 모델은 전력 계통의 그리드, 통신 네트워크, 신경망, 사회 안전망, 수송망과 같은 실제 생활을 모델로 네트워크를 구성한다.

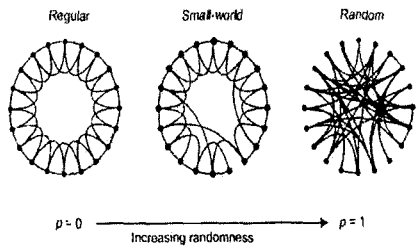


그림 1. 정규 네트워크, small world, 랜덤 네트워크 비교

2-2. Chua's 오실레이터회로를 이용한 Small World 구성

본 연구에서는 그림 1과 같은 Small World 네트워크 구성을 위해 먼저 그림 2와 같은 Chua's 오실레이터회로를 고려하였다.

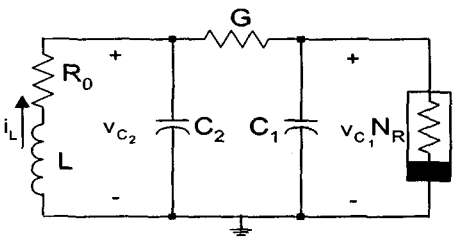


그림 2. Chua's 회로

그림 2의 상태 방정식은 다음과 같이 표현된다.

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

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

$$L\frac{di_L}{dt} = -v_{c_2} + R_0 i_L$$

여기서 v_{c_1}, v_{c_2}는 각각 캐패시터 C_1, C_2의 양단 전압, i_L은 인덕터 L에 흐르는 전류, $G=1/R$, g (·)는 비선형 저항으로써 식(2)와 같이 표현되는 3구분 선형함수(3 segment piecewise-linear function)이다.

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

여기서 m_0는 외부 영역의 기울기, m_1은 내부 영역의 기울기, $\pm B_p$는 break-point이다.

그림2의 Chua's 오실레이터 회로를 이용하여 그림 3과 같은 방식으로 small world 네트워크를 구성하였다.

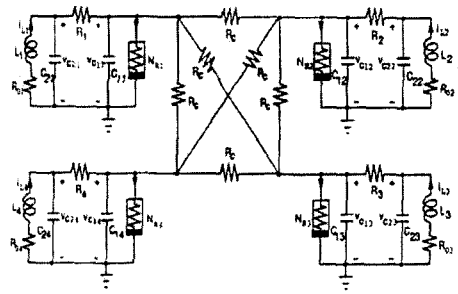


그림 3. Chua's 회로를 이용하여 구성한 Small World 네트워크

그림 3의 상태 방정식에 대한 일반식을 유도하면 식(3)과 같다.

$$C_{1j}\frac{dv_{c_{1j}}}{dt} = G_j(v_{c_{2j}} - v_{c_{1j}}) - g(v_{Rj})$$

$$C_{2j}\frac{dv_{c_{2j}}}{dt} = G_{j(v_{c_{1j}}} - v_{c_{2j}}) + i_{Lj} \qquad (3)$$

$$L_j\frac{di_{Lj}}{dt} = -v_{c_{2j}} + R_{0j} i_{Lj}$$

여기서 비선형 저항의 일반식은 식(4)와 같이 표현할 수 있다.

$$g(v_R) = m_0 v_{Rj} + \frac{1}{2}(m_1 - m_0)[|v_{Rj} + B_p| - |v_{Rj} - B_p|] \qquad (4)$$

여기서, j=1,2,3,4이다.

3. Small World 구축을 위한 비밀 통신 기법

비밀통신을 위해서 그림 3의 회로에 첫 번째 단과 마지막단의 각 단자의 신호가 정확하게 일치하는 동기화가 선행되어야 한다. 그림 3에서 결합 동기를 이루기 위한 상태 방정식은 다음과 같다.

송신부의 상태 방정식

$$C_{11}\frac{dv_{c_{11}}}{dt} = G_1(v_{c_{21}} - v_{c_{11}}) - g(v_{R1})$$

$$+ R_c(-3v_{c_{11}} + v_{C_{12}} + v_{C_{13}} + v_{C_{14}})$$

$$C_{21}\frac{dv_{c_{21}}}{dt} = G_{1(v_{c_{11}}-v_{c_{21}})} + i_{L1} \quad (5)$$

$$L_1\frac{di_{L1}}{dt} = -v_{c_{21}} + R_{0j}i_{L1}$$

제2단 전송부의 상태 방정식

$$C_{12}\frac{dv_{c_{12}}}{dt} = G_2(v_{c_{22}}-v_{c_{12}}) - g(v_{R2}) + R_c(v_{c_{11}}-3v_{C_{12}}+v_{C_{13}}+v_{C_{14}})$$

$$C_{22}\frac{dv_{c_{22}}}{dt} = G_{2(v_{c_{12}}-v_{c_{22}})} + i_{L2} \quad (6)$$

$$L_2\frac{di_{L2}}{dt} = -v_{c_{22}} + R_{0j}i_{L2}$$

제3단 전송부의 상태 방정식

$$C_{13}\frac{dv_{c_{13}}}{dt} = G_3(v_{c_{23}}-v_{c_{13}}) - g(v_{R3}) + R_c(v_{c_{11}}+v_{C_{12}}-3v_{C_{13}}+v_{C_{14}})$$

$$C_{23}\frac{dv_{c_{23}}}{dt} = G_{3(v_{c_{13}}-v_{c_{23}})} + i_{L3} \quad (7)$$

$$L_3\frac{di_{L3}}{dt} = -v_{c_{23}} + R_{0j}i_{L3}$$

수신부의 상태 방정식

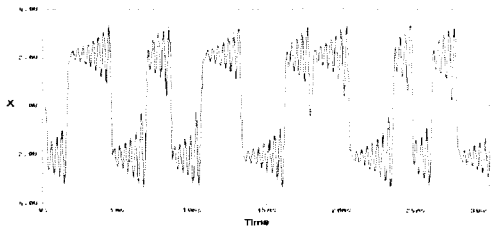
$$C_{14}\frac{dv_{c_{14}}}{dt} = G_4(v_{c_{24}}-v_{c_{14}}) - g(v_{R4}) + R_c(v_{c_{11}}+v_{C_{12}}+3v_{C_{13}}-3v_{C_{14}})$$

$$C_{24}\frac{dv_{c_{24}}}{dt} = G_{4(v_{c_{14}}-v_{c_{24}})} + i_{L4} \quad (8)$$

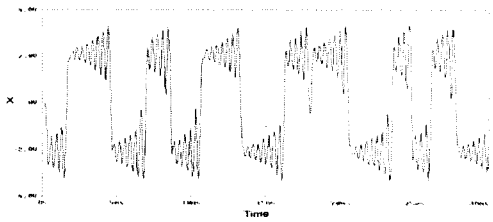
$$L_4\frac{di_{L4}}{dt} = -v_{c_{24}} + R_{0j}i_{L4}$$

여기서 R_c는 선형 결합 저항기의 저항값, j =1,2,3,4에 대하여 $C_{1j}=C_1$, $C_{2j}=C_2$, $L_j=L$, $R_{0j}=R_0$, $R_j=R$, $N_{Rj}=N_R$이다.

식(5)-(8)을 이용하여 그림 3과 같은 small world 네트워크가 안정하기 위한 R_c값을 안정도 이론을 적용하여 계산하면 그림 4와 같은 동기화 결과를 얻는다.



(a) v_{c1}단의 시계열 데이터(송신부)



(b) v_{c4}단의 시계열 데이터(수신부)

그림 4. 송수신부의 동기화 결과

식(5)의 송신부에 그림 5와 같은 구형파의 정보 신호를 삽입하였다.

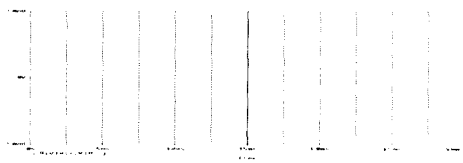


그림 5. 정보 신호

그림 5의 정보 신호를 그림4의 (a)와 같은 송신부의 small world에서 발생한 신호에 합성하면 그림 6과 같은 합성된 신호를 얻을 수 있다.

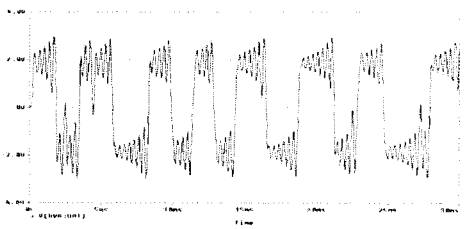


그림 6. 정보 신호와 small world 회로의 수신부 신호와의 합성 신호

Small world의 수신부에서 복조기를 이용하여 복원한 복원 신호를 그림 7에 나타내었다.

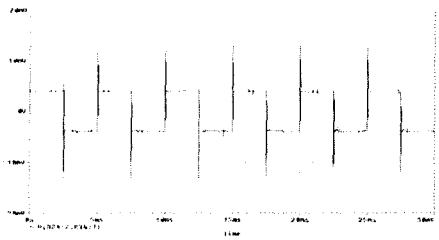


그림 7. 복원 신호

그림 7에서 정보 신호를 복원하였음을 확인할 수 있다. 그림 7의 신호를 필터를 이용하여 필터링 한 결과를 그림 8에 나타내었으며 정보신호와 복원된 복조 신호를 비교한 결과를 그림 9에 나타내었다.

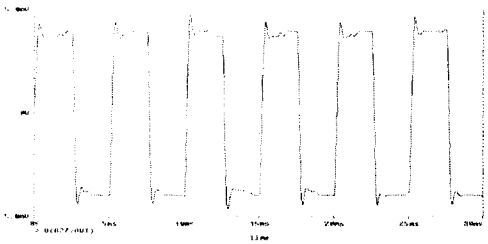


그림 8. 필터링한 정보 신호

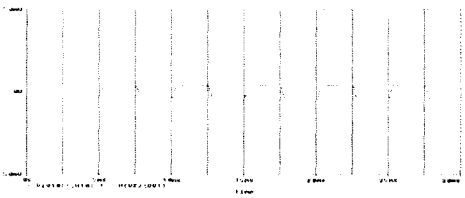


그림 9. 복원 신호

그림 10에서 small world 송신단의 정보 신호와 수신단의 복원신호가 일치함을 확인 할 수 있으며. 이 결과 그림 3과 같은 small world 시스템에서 비밀 통신이 이루어졌음을 확인 할 수 있다.

4. 결 론

본 연구에서는 small world 구축을 위한 비밀 통신 기법을 제시하고 그 결과를 검증하였다. small world 구축을 위한 회로로 Chua's 오실레이터 회로를 이용하였으며 4단을 결합 동기 방식으로 적용하여 동기화 하고 정보신호를 삽입한 후 복조하였다. 앞으로 보다 강건한 비밀 통신 기법이 과제로 남는다.

참고문헌

[1] Cohen,J.E, Briand, F & Newman, C.M, "Community Food Webs: Data and Theory", Springer, Berlin, 1990.

[2] Williams, R.J. & Martinez, N.D, " Simple Rules yield complex food web", Nature, 404, pp.180-183, 2000.

[3] Kohn, K. W, " Molecular interaction map of the mammalian cell cycle control and DNA repair systems", Mol. Biol. Cell. 10, pp. 2703-2734, 1999.

[4] Hartwell, L. H., Hopfield, J.J, Leibler, S & Murray, A, W," From molecular to modular cell biology", Nature, 402, pp. C47-C52, 1999.

[5] Bhalla, U.S & Iyengar, R." Emergent properties of networks of biological signalling pathways", Science, 283, pp.381-387, 1999.

[6] Jeonh-H., Tomber, B., Albert, R., Oltavi, Z.N. & Barabasi, A-L. "Large scale organization of metabollic networks", Nature 407, pp. 651-654, 2000.

[7] Broder, A et al, "Graph structure in the web", Comput. Netw. 33, pp. 309-320, 2000.

[8] Faloutsos, M., Faloutsos, P. & Faloutsos, C, "On power law relationships of the internet topology", Comp. Comm. Rev. 29, pp.251-262. 1999.

[9] Newman, M. E. J., "The structure of scientific collaboration networks", Proc. Natl. Sci, USA 98, pp.404-409, 2001.

[10] Abello, J., Buchsbaum, A & Westbrook, J." A functional approach to external graph algorithms, Lect. Notes Comput. Sci, 1461, pp. 332-343, 1998.

[11] Steven H. Strogatz," Exploring complex networks", Nature. 410, pp. 268-276, 2001.

[12] L.A.N Amaral, A. Scala, M. Barthelemy, & H.E Stanley," Classes of small-world networks", Proc. Natl. Sci, USA 97, pp.11149-11152, 2000.

[13] Debra, S. Goldberg and Frederick P. Roth, " Asscssing experimentally derived interactions in a small world" Proc. Natl. Sci, USA 100, pp.4372-4376. 2003.