Regular paper

Journal of the KIECS. pp. 747-754, vol. 12, no. 5, Oct. 31 2017, t. 85, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.5.747

카오스 기반 Malasoma 시스템의 동기화 및 보안 통신 응용

장은영*

Synchronization and Secure Communication Application of Chaos Based Malasoma System

Eun-Young Jang*

요 약

카오스 기반 보안 통신시스템은 표준 대역확산 시스템의 대안으로서, 이것은 정보신호의 대역을 확산시키며 단순하고 작은 비용으로 카오스회로를 사용하여 정보신호를 암호화할 수 있다. 보안 통신 분야에서는 Lorenz, Chua, Rossler, Duffing등과 같은 전통적인 시스템들이 널리 사용되고 있다. Malasoma 카오스 시스템은 위상학적으로는 단순하지만 불규칙한 신호 생성과 비선형성의 시스템으로서 동기화와 보안 통신을 적용한 시스템은 관련 논문도 거의 없다. 본 논문은 기존의 카오스 시스템의 대안으로서 보안 통신 분야에서 사용될 수 있는 새로운 카오스 시스템을 소개한다. 또한 이 새로운 모델은 시뮬레이션을 통하여 카오스 신호로 보안성을 확인하고 P-C(Pecora-Carroll)방식을 사용하는 동기화 통신시스템을 모델화 한다. Malasoma 시스템의 모델링, 동기화 및 보안 통신 응용은 각각 MATLAB - Simulink 환경에서 구현된다. 이를 통해 도출된 결과는 이 새로운 카오스 시스템이 보안 통신 분야에서 사용될 수 있음을 확인할 수 있다.

ABSTRACT

Chaos-based secure communication systems are alternative of standard spread-spectrum systems that enable spreading the spectrum of the information signals and encrypting information signals with simple and inexpensive chaotic circuitry. In secure communication area, like Lorenz, Chua, Rossler, Duffing etc, classical systems are widely used. Malasoma chaotic system is topologically simple but their dynamical behaviors are non-linear synchronization and secure communication applications has not seen in paper. This paper aims for introducing a new chaotic system which is able to use as alternative to classical chaotic systems into secure communication fields. In addition, this new model simulates a synchronous communication system using P-C (Pecora-Carroll) method by verifying security with chaos signal through simulation. Modelling, synchronization and secure communication applications of Malasoma are realized respectively in MATLAB-Simulink environment. Retrieved results show that this novel chaotic system is able to use in secure communication fields.

키워드

Chaos, Malasoma System, Secure Communication, Peccora-Carroll , Synchronization
카오스, Malasoma 시스템, 보안 통신, Peccora-Carroll, 동기화

* 신라대학교 전자공학과(electronlab@silla.ac.kr)
• 접 수 일 : 2017. 08. 02
• 수정완료일 : 2017. 08. 13
• 게재확정일 : 2017. 10. 18
• Received : Aug 02, 2017, Revised : Aug 13, 2017, Accepted : Oct 18, 2017
• Corresponding Author : Eun-Young Jang
Dept. Electronic Engineering, SILLA University,
Email : electronlab@silla.ac.kr

Ⅰ. 서 론

카오스 신호는 초기조건에 매우 민감하게 반응한다. 또한 카오스 신호는 예측 불가능한 특성을 가지고 있고 광대역 확산으로 잡음 같은 신호를 만들어 낸다. 이러한 신호를 이용하여 신호를 예측할 수 없게 되고 통신 시스템의 보안성을 높일 수 있다. 카오스 기반 보안 통신 시스템은 표준적인 대역 확산 시스템의 대안으로서, 정보 신호의 스펙트럼 확산과 단순하고 저렴한 카오스회로를 사용하여 정보 신호를 암호화 할 수 있게 해준다. 비주기성을 가지고 초기조건의 조그만 변화에도 다른 출력의 신호와 낮은 자기 상관성, 잡음과 유사한 넓은 전력 스펙트럼의 특성은 카오스신호의 가장 중요한 특징들이다[1].

보안 통신을 위하여 카오스 대역 확산신호를 사용하기 위해서는 카오스 시스템의 동기화가 필요하다[2,3]. 동기화 방식중 하나는 Pecora-Carroll (P-C)기법이다. 이 P-C 기법에서 무질서하게 진화하는 시스템으로부터의 상태변수가 기존시스템의 일부분을 복제하여 입력으로서 전송될 때, 이 수신기는 P-C 기법으로 기존의 시스템에 동기화된다. 카오스 동기화에 이 기법을 사용한다면 카오스 시스템은 보안 통신을 구현하는 새로운 방식의 기반역할을 할 수도 있다.

P-C 기법이 제안하는 바는 정보신호를 카오스 신호와 동기화하고 송신기의 서브 시스템 측에서 신호를 안전하게 송신한 후, 수신기 서브 시스템 측에서 복잡한 신호로부터 정보신호를 추출함으로써 성공적으로 카오스동기화를 수행할 수 있다는 것이다 [4].

카오스 시스템의 동기화에 대한 연구는 통신시스템의 설계와 구현을 위한 믿을 수 있고 안전한 통신의 전환점이다. 여러 가지 초기 카오스 기반 보안 통신시스템이 다양한 공격에 대하여 취약한 보안 카테고리를 가지고 있음이 밝혀짐에 따라, “어떻게 하면 발생 가능한 공격에 대응할 수 있는 카오스 - 기반 보안 시스템을 설계할 수 있는지”에 대한 질문이 우리가 직면한 현실적인 도전 과제가 되었다.

Cuomo와 Oppenheim은 카오스 신호를 정보 신호에 추가함으로써 마스킹 목적으로 동기화 개념을 어떻게 사용할 수 있는지 보여주었다 [5]. 그들의 연구는 카오스 신호 동기화를 연구한 통신 논문 중에서 최초의 것이다. Cuomo와 Oppenheim이 자신들의 연구에 로렌츠 (Lorenz) 회로를 사용한 반면, Kocarev와 그의 동료들은 Chua회로를 사용하여 연구를 실시하였다[6].

이러한 선구자적 연구가 실시된 이래 최근까지 여러 연구에서 카오스 시스템의 동기화가 실현되었으며 신뢰할 수 있는 통신을 구현하기 위한 목적의 카오스 시스템 동기화도 실현되었다[7,8].

본 논문의 다음 장에서는 Malasoma 시스템을 사용하는 가장 단순한 카오스 시스템에 대하여 소개하고 있다[9]. 세 번째 장에서는 P-C 방식을 사용하여 이 시스템의 동기화를 구현하였다[10]. 네 번째 장에서는 동기화된 Malasoma 시스템을 사용하는 카오스 정보 보안 통신의 시뮬레이션 결과에 대하여 논의하였다[11-13]. 그리고 마지막 절에서는 전체 연구에 대하여 간략하게 평가하였다.

Ⅱ. 카오스를 사용하는 Malasoma 시스템

카오스 시스템의 동기화와 관련된 연구 또는 통신에서 동기화된 카오스 시스템과 관련된 연구들을 살펴보면, 여러 시스템 중에서 Chua, Lorenz, Rössler, Van Der Pol가 많이 사용되었으며, 그 중에서도 몇몇은 보안 통신 아날로지가 매우 단순한 구조를 가지고 있다. 하지만 본 연구에서 사용된 Malasoma 비선형 방정식 시스템은 매우 불규칙한 카오스 신호를 보여 주고 있으며 다른 방법들보다 더욱 복잡한 구조를 가지고 있다.

Malasoma 비선형 방정식 시스템은 2000년대에 도입 되었으며 식(1)과 같이 나타낼 수 있다.

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -a \cdot z + x \cdot y^2 - x \end{aligned} \tag{1}$$

Malasoma 시스템 회로 시뮬레이션은 Simulink 환경에서 모델링되었으며, 그림 1은 Malasoma 방정식 모델의 블럭도이다. 그림 2은 2차원 Attractor이고 그림 3은 x-y-z 3차원 Attractor의 결과이다.

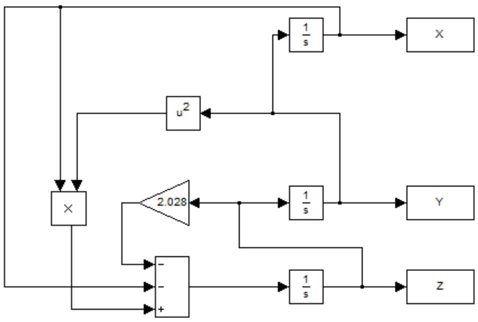
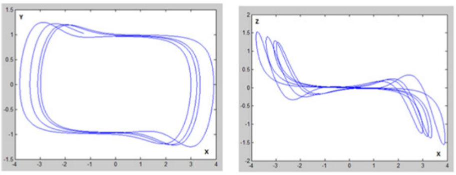
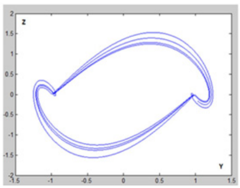


그림 1. Malasoma 시스템의 Simulink 모델
Fig. 1 Malasoma system diagram using Simulink



(a) x-y (b) x-z



(c) y-z
그림 2. Malasoma 시스템에 대한 카오스신호의 attractors
Fig. 2 chaotic attractors for Malasoma system

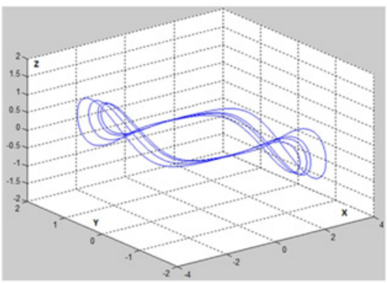


그림 3. Malasoma시스템의 삼차원 x-y-z attractor
Fig. 3 Three-dimensional x-y-z strange attractors of Malasoma system.

이 시스템은 a = 2.028에서의 카오스 attractor을 나타내며, a값에 대한 리아푸노프 지수는 0.738, 0, −3.2142이다. 이 조건은 카오스에 대한 일반적인 주기 경로를 따름으로, 결국 a가 작아지면 경계위기와 무한해가 나타난다. 리아푸노프 지수는 카오스의 특징인 초기 조건에 대한 민감성을 측정한다. 비선형적인 카오스 신호가 나타나는 a의 범위는 2.0278 < a < 2.085로 매우 좁다. 또한 0.07535 < a < 0.07536의 범위에서 두 번째로 작은 카오스 attractor가 나타난다. 이것은 앞의 범위보다 5000배 더 작다.

III. Malasoma 시스템의 동기화

P-C 방식을 Malasoma system의 운동방정식에 적용하면, 그림 4와 같은 동기화 다이어그램을 구할 수 있다[9]. 첫 번째 응답의 x 변수에서 z 변수로가 아닌 드라이브 시스템이 하위 시스템으로 전송될 수 있다.

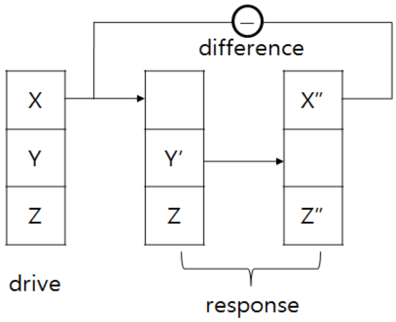


그림 4. P-C 동기화 블록선도
Fig 4. P-C synchronization block diagram

$$\begin{aligned} \dot{x}' &= y' \\ \dot{y}' &= z \end{aligned} \qquad (2)$$

주어진 공식에서 식(2)와 같이 1차 (x', y') 안정 응답-서브시스템으로 만들 수 있다.

그리고 식(2)는 식(3)과 같이 2차 (x'', z'') 안정 응답-서브시스템으로 작성될 수 있다.

$$\begin{aligned} \dot{x}'' &= y' \\ \dot{z}'' &= -a \cdot z'' + y'^2 \cdot x - x'' \end{aligned} \qquad (3)$$

두 개의 카오스 신호의 카오스 동기화는 주-종(master-slave) 구성으로 나타남에 따라 서로 간에 연결 되어있다. 주 시스템은 식(1)에서 설명한 방정식으로서 설명될 수 있다. 종 시스템은 주 시스템에 완벽하게 일치하며, 유일한 차이는 (x'', z'') 상수 응답 서브시스템이 시간 생성 신호 z를 사용하는 주 시스템에 의해 구동 된다는 점이다. 그러므로 종 시스템은 식(4)와 같이 표현할 수 있다.

$$\begin{aligned} \dot{x}_r &= y_r \\ \dot{y}_r &= z_r \\ \dot{z}_r &= -a \bullet z = x_r \bullet y_r^2 - x_r \end{aligned} \qquad (4)$$

파라미터 z와 z_r이 동일하다면, 신호는 정확히 동일 할 것이다. 동기화는 주 시스템 과 종 시스템 사이의 작은 에러 값을 확인할 수 있다. Simulink을 사용하여 초기 조건이 서로 차이가 있는 두 개의 시스템의 시뮬레이션을 하였다. 각각(x_0, y_0, z_0) = (0, 0.96, 0)과 (x_0, y_0, z_0) = (0.00005, 0, −0.67499)의 두 개의 시스템과 a의 값은 2.028 이다. 시뮬레이션을 위하여 비동기적인 서로 다른 초기 조건으로 실행한 후 , 신호들의 z상태변수 및 z_c값의 상호간의 변화를 그림 5에서 확인할 수 있고 그림 6에서 두 신호의 차이 값을 에러로 확인 할 수 있다. 이런 에러로 카오스 시스템이 초기 조건에 매우 민감하다는 것을 증명할 수 있다.

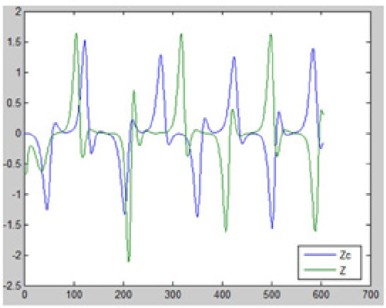


그림 5. Drive신호 (z), Response신호 (z_c)
Fig. 5 driving signal(z) and response signal (z_c)

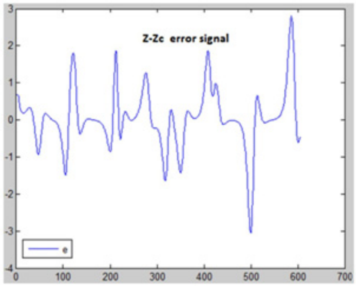


그림 6. 동기화 전의 z-z_c차이값
Fig. 6 z-z_c difference signal before synchronization phase (error signal).

그림 7은 두 시스템의 Malasoma 시스템의 P-C 동기화방식의 초기 Simulink 블록선도이다. 초기 값 (x_0, y_0, z_0) = (0, 0.96, 0) 이다.

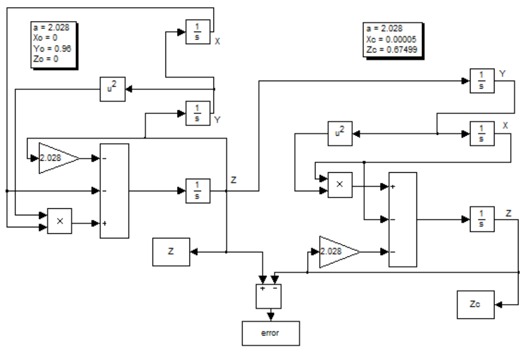


그림 7. Malasoma시스템의 Simulink P-C 동기화모델링
Fig. 7 Simulink P-C synchronization modelling of Malasoma system.

시뮬레이션이 시작된 후 드라이브 신호 z와 응답 신호 z_c가 매우 짧은 시간 내에 동기화 되는 것이 그림 8에서 확인할 수 있다.

그림 9는 z에서 z_c를 빼서 차이 (e = 에러) 신호이다. 동기화 시스템은 매우 짧은 시간동안 0이 아닌 다른 값들을 가진 후 에러값은 0이 된다. 따라서 송신 및 수신회로는 1 ~ 2 ms 정도의 매우 짧은 시간 안에 완전히 동기화 되는 것을 확인할 수 있다.

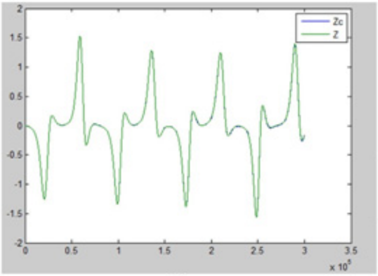


그림 8. z 와 z_c값의 변화

Fig. 8 Changes of z and z_c

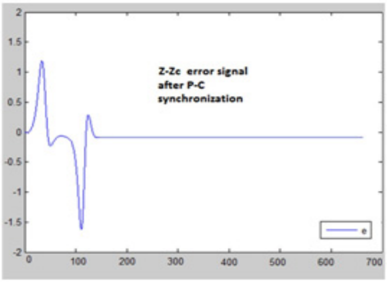


그림 9. 동기화 후의 $z-z_c$ 차이값

Fig. 9 difference signal after synchronization phase

Ⅳ. Malasoma 시스템의 카오스 보안 통신 모델링

송신기 회로방정식은 다음과 같다.

$$\begin{aligned} \dot{x}_c &= y_c \\ \dot{y}_c &= s(t) \\ \dot{z}_c &= -a \cdot s(t) + x_c \cdot y_c^2 - x_c \end{aligned} \qquad (5)$$

카오스 정보 암호화 통신방식의 기본 블럭도는 그림 10과 같다. 정보신호는 0.04V 사인파 신호로서 사용된다. $i(t)$ 정보신호와 카오스신호 $z(t)$가 합쳐지며 송신수단으로 전달된다.

송신된 $s(t)$ 신호는 이 두 가지 신호의 합이다. 수신기에서는 $z(t)$신호와의 실제 동기화에 따라 P-C 방식이 동일한 형태로 이루어지며, 송신된 $s(t)$로부터 동기화된 $z_c(t)$ 카오스 신호가 제거되어, 결국 $i_c(t)$ 정보신호를 다시 얻게 된다.

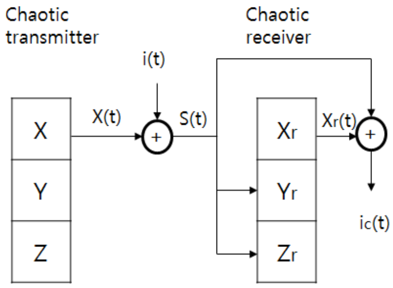


그림 10. 카오스 정보 암호화 통신 방식의 블록도

Fig. 10 Principle scheme for chaotic information hiding communication method

그림 11은 P-C 동기화방식으로 Malasoma 시스템을 사용하는 카오스 보안 통신 블록도이다.

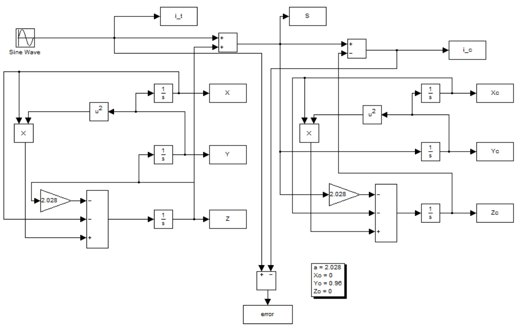
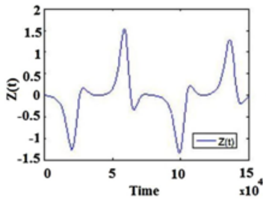


그림 11. Simulink 이용한 Malasoma 카오스 암호화 통신방식

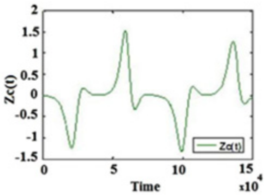
Fig. 11 Chaotic information hiding communication method of Malasoma using Simulink

카오스신호를 사용하여 통신에서 정보를 암호화하는 방식에서 요구하는 것은 정보신호의 진폭이 카오스신호의 진폭보다 더 작아야한다는 것이다. 모든 시스템에 대하여 정보를 표시하기 위하여 0.4 V 또는 1V 진폭을 가지는 사인파를 사용하였다.

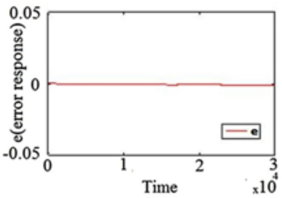
Malasoma 시스템에서 카오스 회로의 출력은 3.5 V 피크-투-피크 전압진폭을 나타낸다. 정보 신호의 완전한 복구를 보장하기 위하여 카오스 정보 암호화 통신방식에서 정보신호는 카오스 신호보다 20dB 더 작아야한다. 그림 12는 정보신호와 에러 값이다.



(a) Transmitter signal $i(t)$



(b) Receiver signal $i_c(t)$



(c) error $(i(t) - i_c(t))$

그림 12. Malasoma 모델링을 사용하는 카오스 보안 통신 방식의 시뮬레이션 결과
Fig. 12 Simulation results of Chaos security communication method using Malasoma modeling

V. 결 론

P-C 동기화 방법이 적용된 Malasoma 시스템을 사용하는 카오스 정보 보안 통신은 아직까지 각종 문헌상에 잘 알려져 있지 않은 새로운 방법이다. 본 연구에서는 동기화와 보안 통신의 시뮬레이션을 통하여, 송신기와 수신기의 에러가 거의 0에 가까운 것을 확인하였고 이 시스템이 보안을 목적으로 통신시스템 사용될 수도 있음을 확인하였다. 추가적인 연구주제로서 통신 분야외의 다른 응용 분야에 적용할 수도 있다.

또한 Malasoma 카오스 attractor를 사용하여 동기화된 보안통신의 회로구현에 대하여 연구할 수도 있다. 이러한 통신회로를 구현한 다음에는 카오스 변조와 카오스 스위칭에 대하여 좀 더 상세하게 연구할 것이다.

References

[1] N. Noroozi, B. Khaki, and A. Seifi, “Chaotic oscillations damping in power system by finite time control,” *Int. Rev. Electr. Eng.-I* vol 3. no 6, May,2 008, pp.1032 - 1038.

[2] A. Ouannas, M. Sawalha, and T. Ziar, “Fractional chaos synchronization schemes for different dimensional systems with non-identical fractional-orders via two scaling matrices,” *Optik* vol. 127. no 20, jun 2016, pp.8410 - 8418.

[3] M. Kennedy and L. Chua, “Van Der Pol and chaos,” *IEEE Trans. Circuits Syst. CAS* vol 33. no 10, oct 1986, pp.974 - 980.

[4] L. Pecora and T. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.* vol. 64. no 8, Feb 1990, pp.821 - 825.

[5] K. Cuomo, A. Oppenheim, and S. Strogatz, “Synchronization of Lorenz-based chaotic circuits with applications to communications,” *IEEE Trans. Circuits-II* vol. 40. no. 10, Oct 1993, pp.626 - 633.

[6] L. Kocarev, K. Halle, K. Eckert, L. Chua, and U. Parlitz, “Experimental demonstration of secure communications via chaotic synchronization,” *Int. J. Bifurc. Chaos.* vol. 2. no 3, Sep 1992, pp.709 - 713.

[7] A. Alexeyev and M. Green, “Secure communications based on variable topology of chaotic circuits,” *Int. J. Bifurc. Chaos.* vol. 7 no 12, Apr 1997, pp.2861 - 2869.

[8] J. Sprott, “Simple chaotic systems and circuits”, *Am. J. Phys.* vol. 68. no 8, Jul 2000, pp.758 - 763.

[9] I. Pehlivan, Y. Uyaroglu “Rikitake Attractor and its synchronization application for secure communication systems,” *J. Appl. Sci.* vol. 7. no 2, Mar 2007, pp.232 - 236.

[10] J. Malasoma, "A new class of minimal chaotic flows,” *Phys. Lett. A.* vol. 305. no 1 - 2, Nov 2002, pp.52 - 58.

[11] E. Jang “Design of digital communication systems using DCSK chaotic modulation,” *J. of Korea Institute of Electronic Communication Sciences*, vol. 10. no 5, May 2015, pp.565 - 570.

[12] E. Jang “Design of FM-QCSK Chaotic Communication System for high-speed communication,” *J. of Korea Institute of Electronic Communication Sciences*, vol 10. no 10, oct 2015, pp.1183 - 1188.

[13] W, Zhang and H, Suh“ International Conference on Communications,” *J. of the Korea*

Institute of Electronic Communication Sciences, vol. 12, no. 1, Feb. 2017, pp. 61-68.

저자 소개

장은영(Eun-Young Jang)

1998년 동아대학교 전자공학과 졸업(공학사)
2000년 동아대학교 대학원 전자공학과 졸업(공학석사)
2008년 동아대학교 대학원 전자공학과 졸업(공학박사)
2014년 ~현재 신라대학교 공과대학 전자공학과 조교수
※ 관심분야 : 무선통신시스템, 5G이동통신 시스템