http://dx.doi.org/10.7840/kics.2014.39A.6.303

보안성 향상을 위한 스크램블링 COOK 변조 방식

이 준 현◆, 이 동 형*, 금 홍 식**, 유 흥 균°

Scrambling Chaotic On Off Keying Modulation Scheme for Security Improvement

Jun-Hyun Lee◆, Dong-Hyung Lee*, Hong-Sik Keum**, Heung-Gyoon Ryu°

요 약

보안성을 향상시킬 수 있는 시스템인 카오스 통신 시스템은 신호의 비예측성, 비주기성, 광대역성, 구현의 용이성 등의 특징을 가지며, 초기조건에 굉장히 민감한 특징을 가진다. 이런 특징들로 인해서 카오스 통신 시스템의 보안성은 디지털 통신 시스템보다 우수하다. COOK 변조 방식은 비동기식 수신기를 사용하면서도 다른 카오스 변조 방식보다 BER 성능이 우수하게 평가된다. 하지만 COOK 변조 신호는 정보 비트의 예측이 쉽기 때문에 보안성과 신호의 안전성 측면에서는 다른 카오스 변조 방식보다 나쁘게 평가된다. 따라서 본 논문에서, 우리는 COOK 변조 방식의 보안성과 신호의 안전성을 향상시키기 위해 스크램블링 기법을 응용하여 새로운 스크램블링 COOK 변조 방식을 제안한다. 기존 COOK 변조 방식은 데이터가 1인 경우에만 카오스 신호를 발생시키기 때문에 데이터 예측이 가능하지만, 스크램블링 COOK 변조 방식은 발생된 카오스 신호가 0일 수도 있으며 1일 수도 있기 때문에 예측이 불가능하다. 따라서 스크램블링 COOK 변조 방식은 기존 COOK 변조 방식보다 전송 신호의 보안성과 안전성을 향상시킬 수 있다.

Key Words : COOK system, Scrambling algorithm, Security, Chaos communication

ABSTRACT

Chaos communication system can improve a system security due to characteristics of non-periodic, non-predictability, broadband signal and easy implementation. Also, chaos signal is sensitive to initial conditions of chaos map. By these reasons, security of chaos communication system is superior to digital communication system. BER performance of COOK modulation system is better than other chaos modulation systems, even if COOK modulation system uses an asynchronous receiver. However, security and safety of COOK modulated signal are worse than other chaos modulation systems, because information bits can be easily predicted from COOK modulated signal. In this paper, for security improvement of COOK modulated signal, we propose a novel Scrambling COOK modulation system by applying the scrambling method. Conventional COOK modulated signal can be predicted, because chaos signal is generated when data is only 1. However, proposed system cannot be predicted, because chaos signal is generated when data is 0 or 1. Therefore, security and safety of transmitted signal in scrambling COOK modulation system is superior to conventional COOK modulation system.

※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2012017339)
◆ First Author : Department of Electronic Engineering, Chungbuk National University, toogee89@nate.com, 학생회원
° Corresponding Author : Department of Electronic Engineering, Chungbuk National University, ecomm@cbu.ac.kr, 정회원
* SK Telecom, danny92@nate.com, 정회원
** 한국전파진흥협회, hskeum@rapa.or.kr, 정회원
논문번호 : KICS2014-03-098, Received March 21, 2014; Revised June 3, 2014; Accepted June 3, 2014

Ⅰ. 서 론

기존의 디지털 통신 연구는 선형 시스템에 대해서 활발하게 이루어졌다. 하지만 선형 시스템의 성능 향상에 대한 연구가 기본적인 한계에 부딪치게 되면서 비선형 통신 시스템에 대한 연구가 활발히 이루어지기 시작하였다[1]. 최근, 전기통신의 고도화에 따라 무선통신의 이용도는 날이 갈수록 증가하고 있으며, 다양한 정보의 교류도 급속히 증가하고 있다. 통신기술의 고도화는 곧 정보수집수단의 고도화로 연결되며 적의 도청 능력이나 해킹 수준이 높아지고 있다. 또한, 무선 통신은 취약성이 많으며 장거리에서 쉽게 도청이 가능하기 때문에 통신 시스템의 보안성에 대한 연구는 굉장히 활발하게 진행되고 있으며 중요한 연구과제로 분류되고 있다[2].

무선 통신 시스템에서 신호의 보안성을 향상시킬 수 있는 방법 중에 하나는 카오스 신호를 이용한 카오스 통신 시스템이 있다[2,3]. 카오스 통신 시스템은 대역 확산 기법을 사용하며, 카오스 신호를 이용하여 신호를 예측할 수 없게 만들어 통신 시스템의 보안성을 향상시킨다. 카오스 통신 시스템은 신호의 비예측성, 비주기성, 광대역성, 구현의 용이성 등의 특징을 가지며, 초기조건에 굉장히 민감한 특징을 가진다. 카오스 신호는 비선형적이며, 불규칙하게 생성되는데, 초기조건이 미세하게 변하더라도 완전히 다른 신호로 변하기 때문에 초기조건에 굉장히 민감한 특징을 가진다[4]. 또한, 신호가 카오스 신호에 의해 확산되어 전송되므로 중간에서 신호 감지가 어렵고, 전파 방해에 강하다는 특징을 가지며, 도청 확률을 줄일 수 있다. 이런 특징들로 인해서 카오스 통신 시스템의 보안성을 디지털 통신 시스템보다 우수하게 평가된다[5]. 이런 카오스 통신 시스템의 특징으로 인해, 카오스 시스템은 군용 통신에 적용이 가능하며, 이에 대한 연구가 활발히 이루어지고 있다. 또한, 통신 암호화 기법으로 활용하기 위한 연구가 진행 중이다.

카오스 통신 시스템에는 여러 변조 방식이 존재하며, 각 변조 방식에 따라 성능과 보안성이 다르게 평가된다. 카오스 시스템은 대표적으로 2가지의 수신기로 구성되는데, 하나는 동기식 수신기이며 다른 하나는 비동기식 수신기이다. 동기식 수신기는 수신된 데이터를 복구하기 위해서 완벽한 카오스 신호의 동기가 필요한 수신기를 의미하며, 비동기식 수신기는 카오스 신호의 동기가 필요 없는 구조의 수신기를 의미한다. 일반적으로 동기식 수신기를 사용하면 비동기식 수신기를 사용하는 것보다 BER 성능이 좋게 평가된다. 하지만 카오스 신호는 초기 조건에 굉장히 민감한 특징을 가지고 있기 때문에 카오스 신호의 동기를 완벽하게 맞추는 것은 어려운 일이다[6]. 비동기식 수신기를 사용하는 카오스 변조 방식으로는 COOK, DCSK, CDSK 변조 방식이 있는데, 3가지의 변조 방식 중에서는 COOK 변조 방식이 가장 좋은 BER 성능을 갖는다[7,8].

하지만 COOK 변조 방식은 정보 비트가 1인 경우에만 카오스 신호를 전송하기 때문에 전송 신호를 보면 정보 비트를 쉽게 예측할 수 있다. 이런 이유로 인해서 다른 카오스 변조 방식보다 전송 신호의 보안성과 안전성이 나쁘게 평가된다[9]. 따라서 COOK 변조 방식에서 전송 신호의 보안성과 안전성을 향상시킬 수 있다면, 다른 카오스 변조 방식보다 더 좋은 BER 성능을 가지면서, 보안성도 좋은 카오스 변조 방식으로 재구성을 할 수 있다. 이런 이유로 인해 COOK 변조 방식의 보안성과 안전성 향상에 대한 연구는 굉장히 중요하다.

본 논문에서 COOK 변조 방식의 전송 신호를 예측할 수 있다는 단점을 해결하기 위해 스크램블링 기법을 적용시킨다. 스크램블링 기법을 적용함으로써 제 3자가 전송된 카오스 신호가 0인지 1인지를 알 수 없게 만들어서, 신호의 보안성과 신호의 안전성을 향상시킬 수 있다. 따라서 우리는 스크램블링 기법을 적용하여 새로운 스크램블링 COOK 변조 방식을 제안한다. 우리가 제안한 이 시스템은 기존 COOK 변조 방식보다 BER 성능 열화없이 데이터의 보안성을 향상시킬 수 있다.

Ⅱ. System Overview

2.1 Chaotic On Off Keying System

COOK(Chaotic On Off Keying) 변조 방식은 동기식 수신기나 비동기식 수신기를 모두 사용할 수 있는 시스템이다. 카오스 신호는 초기 조건에 민감한 특징이 있기 때문에, 카오스 신호 동기가 하드웨어적으로 구현이 어렵다. 이런 이유로 인해, 실제로 시스템을 구현할 때는 비동기식 수신기를 많이 사용한다. COOK 변조 방식은 스위치로 제어되는 특징을 가지며, 전송되는 심볼들 사이의 거리를 최대화할 수 있는 장점을 가진다[7].

그림 1은 COOK 변조 방식의 송신기를 나타낸다. 데이터가 1인 경우에는 스위치가 닫힌 상태가 되고 카오스 신호가 전송된다. 그리고 데이터가 0인 경우에는 스위치가 열린 상태가 되고 아무런 신호를 전송하

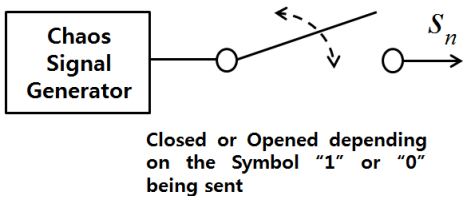

그림 1. COOK 변조 방식의 송신기.
Fig. 1. Transmitter of COOK modulation system.

지 않는다.

$$S_n(t) = \begin{cases} c_n(t) & Data = 1 \\ 0 & Data = 0 \end{cases} \quad (1)$$

식(1)는 COOK 변조 방식의 전송 신호를 수식으로 나타낸 것이다. $c(t)$는 카오스 신호 생성기에서 생성된 카오스 신호를 의미한다. 그리고 스위치는 데이터 0과 1에 의해 제어된다.

COOK 변조 방식에서, 데이터는 동기식 수신기나 비동기식 수신기를 사용함으로써 복구할 수 있다. 그림 2는 COOK 변조 방식의 수신기를 나타낸다. 수신기에서는 수신된 신호의 제곱을 확산인자만큼 더해준 후에 임계값을 통해 데이터를 복구할 수 있다.

$$y_n(t) = \begin{cases} \sum_{t=1}^{M} r_n^2(t) & Data = 1 \\ 0 & Data = 0 \end{cases} \quad (2)$$

식(2)는 수신 신호의 상관기 출력을 수식으로 나타낸 것이다. 일반적으로 디지털 통신 시스템에서는 임계값 0을 기준으로 판단을 하지만, COOK 변조 방식에서는 $E\left[\sum_{t=1}^{M} r^2(t)\right]$와 0의 중간 값이 임계값으로 설정된다. 그래서 임계값보다 크면 심볼은 1로 복구되고, 작으면 0으로 복구된다.

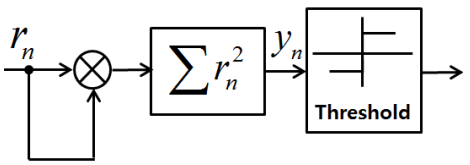

그림 2. COOK 변조 방식의 수신기.
Fig. 2. Receiver of COOK modulation system.

2.2 Chaos map

카오스 신호는 카오스 맵 방정식에 의해 생성된다. 본 논문에서 사용한 카오스 맵은 Logistic map이며, Logistic map의 궤적은 그림 3과 같이 그려진다.

$$x_{n+1} = Rx_n(1-x_n) \quad (3)$$

Logistic map은 선형적인 특징과 비선형적인 특징을 모두 가지며, 이전의 출력값을 현재의 입력값으로 사용하는 방정식을 가진다. Logistic map의 방정식은 식(3)으로 표현되며, 매개 변수 R의 값이 3.9999일 때, 그림 1과 같은 궤적을 그린다. 그리고 그림 1의 x축은 x_n이며 y축은 x_{n+1}을 의미한다.

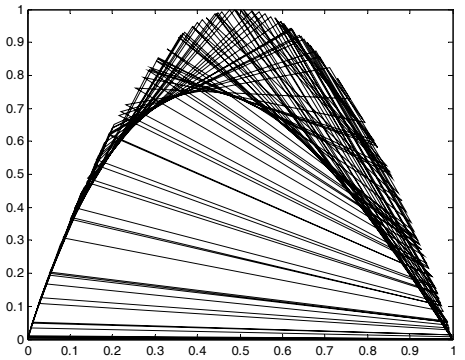

그림 3. Logistic map의 궤적.
Fig. 3. Trajectory of Logistic map.

Ⅲ. Scrambling Chaotic On Off Keying System

그림 4는 데이터가 [01010001101001010101]일 때, COOK 변조 방식의 전송 신호를 나타낸 것이다. 그림 4를 보면 알 수 있듯이, 제 3자(해커)가 전송된 신호를 가로챈다면 다른 카오스 통신 시스템에 비해서 데이터의 복원이 쉽기 때문에 보안성이나 신호의 안전성 측면에서 다른 카오스 변조 방식보다 좋지 않게 평가된다. 이런 이유로 인해, COOK 변조 방식의 전송 신호의 안전성을 더 향상시킬 필요가 있다. 그래

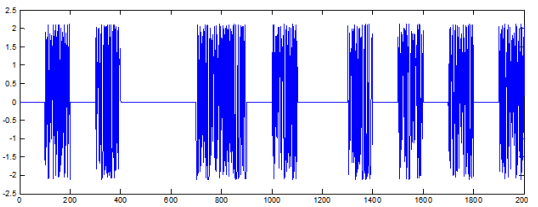

그림 4. COOK 변조 방식의 전송 신호.
Fig. 4. Transmission signal of COOK modulation system.

서 우리는 스크램블링 기법을 기존 시스템에 적용함으로써 새로운 스크램블링 COOK 변조 방식을 재구성한다.

$$S_n(t)=\begin{cases} c_n(t) & Data=1, B_{n,switch}=1 \\ 0 & Data=0, B_{n,switch}=1 \\ 0 & Data=1, B_{n,switch}=0 \\ c_n(t) & Data=0, B_{n,switch}=0 \end{cases} \quad (4)$$

그림 5는 우리가 제안한 스크램블링 COOK 변조 방식의 송신기를 나타낸다. 기존 COOK 변조 방식은 데이터가 1인 경우에만 카오스 신호를 전송한다. 하지만 제안한 스크램블링 COOK 변조방식에서는 스크램블링 비트에 따라 데이터가 1이거나 0일 때에도 카오스 신호를 전송한다. 스크램블링 비트는 송신단과 수신단이 서로 공유하고 있는 비트를 의미한다. 제안한 스크램블링 COOK 변조 방식에서는 스크램블링 비트가 1인 경우에 기존 COOK 변조 방식처럼 데이터가 1일 때 카오스 신호를 전송한다. 하지만 스크램블링 비트 0인 경우에는 반대로 데이터가 0일 때 카오스 신호를 전송한다. 데이터가 1인 경우에만 카오스 신호를 전송하는 것이 아니기 때문에 제 3자(해커)가 전송된 신호를 가로채더라도 스크램블링 비트를 모른다면 데이터를 완벽하게 복구할 수 없다. 따라서 제안한 스크램블링 COOK 변조 방식의 보안성이나 신호의 안전성은 기존 COOK 변조 방식보다 향상된다고 평가할 수 있다.

식(4)는 제안한 스크램블링 COOK 변조 방식의 송신 신호를 나타낸다. $B_{n,switch}$는 스크램블링 비트를 나타낸다. 즉, 스크램블링 비트를 통해서 데이터를 혼란시킨 후에 카오스 신호를 전송한다.

그림 6은 스크램블링 COOK 변조 방식의 수신기를 나타낸다. 기존 COOK 변조 방식과 비슷하지만 송신기에서 사용한 스크램블링 비트을 고려하여 데이터

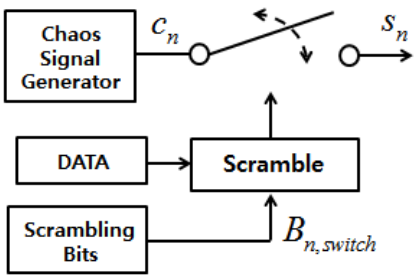

그림 5. 스크램블링 COOK 변조 방식의 송신기.
Fig. 5. Transmitter of Scrambling COOK modulation system.

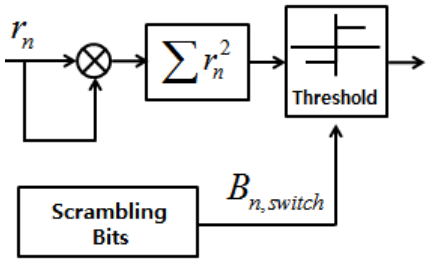

그림 6. 스크램블링 COOK 변조 방식의 수신기.
Fig. 6. Receiver of Scrambling COOK modulation system.

를 복구해야한다.

$$\begin{cases} \sum_{t=1}^{M} r_n^2(t), B_{n,switch}=1 & Data=1 \\ 0, B_{n,switch}=1 & Data=0 \\ 0, B_{n,switch}=0 & Data=1 \\ \sum_{t=1}^{M} r_n^2(t), B_{n,switch}=0 & Data=0 \end{cases} \quad (5)$$

식(5)는 Threshold 과정에서의 비트 판정을 나타낸다. 스크램블링 비트가 1일 때, 데이터는 기존 COOK 변조 방식과 동일하게 임계값에 따라 데이터가 복구된다. 하지만 스크램블링 비트가 0일 때, 데이터는 기존 COOK 변조 방식과는 반대로 임계값보다 크면 0으로 복원되며, 작으면 1로 복원된다.

Ⅳ. 성능 평가

COOK 변조 방식은 동기식 수신기와 비동기식 수신기 모두 사용 가능하다. 본 논문에서는 비동기식 수신기를 사용하여 데이터를 복원한다. 같은 비동기식 수신기를 사용하는 CDSK 변조 방식이나 DCSK 변조 방식의 BER 성능보다 COOK 변조 방식의 BER 성능은 일반적으로 좋게 평가된다. 본 연구는 Matlab을 통해 카오스 변조 시스템을 구성하고 AWGN 환경에서 성능을 평가하였다.

그림 7은 비동기식 수신기를 사용하는 카오스 변조 방식인 CDSK와 DCSK, COOK 변조 방식의 BER 성능을 비교한 것이다. 그림 7을 보면, COOK 변조 방식의 BER 성능이 DCSK나 CDSK 변조 방식보다 월등히 좋은 것을 알 수 있다[3]. 하지만 COOK 변조 방식은 전송신호로 데이터를 예측할 수 있는 단점을 가진다. 따라서 COOK 변조 방식에서 송신 신호의 안전성을 향상시킬 수 있다면 DCSK나 CDSK 변조 방식보다 더 좋은 시스템으로 재구성할 수 있다.

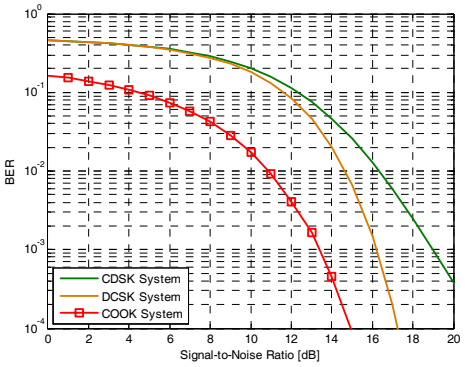

그림 7. COOK 변조 방식의 BER 성능.
Fig. 7. BER performance of COOK system in AWGN.

그림 8은 스크램블링 COOK 변조 방식의 전송 신호를 나타낸다. 전송하고자하는 정보 비트는 [0101110011]이지만 카오스 신호는 불규칙하게 전송된다는 것을 알 수 있다. 기존 COOK 변조 방식은 전송 신호를 보면 정보 비트를 예측할 수 있었지만, 스크램블링 COOK 변조 방식의 전송 신호는 정보 비트를 예측할 수 없다. 따라서 스크램블링 비트를 통해 데이터를 혼합해주고, 이로 인해 데이터의 보안성과 신호의 안전성을 향상시킬 수 있다.

본 논문에서의 스크램블링 비트는 단순히 0과 1로 이루어진 비트로 생성했으며, 20개의 비트를 반복하여 생성하였다. 그림 9는 송수신단이 모두 스크램블링 비트를 정확히 알고 있을 때의 BER 성능을 나타낸다. 그림 9를 보면 스크램블링 비트의 동기가 완벽하다면 BER 성능 열화 없이 보안성과 신호의 안전성을 향상시킬 수 있다. 스크램블링 비트는 특정 비트를 반복할 수 있지만, 카오스 신호를 이용할 수 있다. 카오스 신

Scrambling Bits : 0 0 1 1 0 0 0 0 1 0
Information Bits : 0 1 0 1 1 1 0 0 1 1

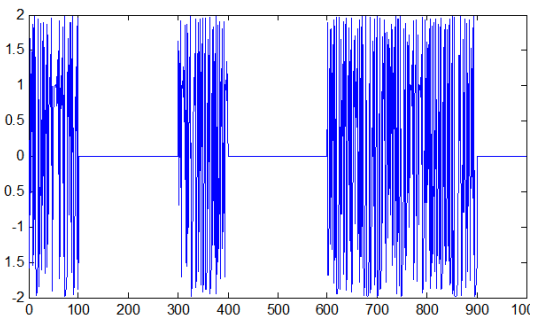

그림 8. 스크램블링 COOK 변조 방식의 전송 신호.
Fig. 8. Transmission signal of Scrambling COOK modulation system.

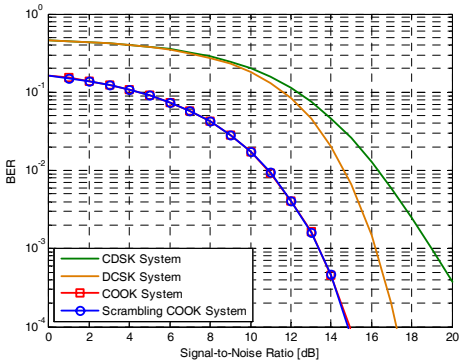

그림 9. 스크램블링 COOK 변조 방식의 BER 성능.
Fig. 9. BER performance of Scrambling COOK system in AWGN.

호의 부호가 +인 경우에는 1로, -인 경우에는 0으로 출력한다면 스크램블링 비트로 사용이 가능하다. 하지만 카오스 신호의 부호에 대한 동기를 완벽하게 맞춰야 한다. 카오스 신호는 초기 조건에 따라 완전히 다른 신호로 변하므로 특정비트보다 더 예측이 불가능하고, 이로 인해 특정 비트의 반복인 경우보다 좀 더 향상된 보안성과 신호의 안전성을 얻을 수 있다.

V. 결 론

본 논문에서 우리는 COOK 변조 방식의 보안성과 신호의 안전성을 향상시키기 위해 스크램블링 COOK 변조 방식을 제안했다. 기존 COOK 변조 방식은 데이터가 1인 경우에만 카오스 신호를 발생시키는 구조로 되어있다. 반면에 제안한 스크램블링 COOK 변조 방식은 스크램블링 비트를 사용함으로써, 발생된 카오스 신호가 데이터 0을 의미하는지 1을 의미하는지 알 수 없게 만든다. 스크램블링 비트는 송수신단에서 정확히 알고 있어야하며, 정확히 동기가 이루어지면 BER 성능 열화없이 기존 COOK 변조 방식보다 데이터의 보안성과 안전성을 향상시킬 수 있다. 또한, 카오스 신호의 부호에 대한 동기를 완벽하게 맞출 수 있다면 카오스 신호를 스크램블링 비트로 사용할 수 있고, 이 경우에는 특정 비트로 생성했을 때보다 좀 더 향상된 보안성과 신호의 안전성을 얻을 수 있다.

References

[1] N. F. Rulkov and M. M. Sushchik, “Digital communication using chaotic pulse position modulation,” *IEEE Trans. Circuits Syst.,* vol.

48, pp. 1436-1444, 2001.

[2] C. Guyeux, N. Friot, and J. M. Bahi, "Chaotic iterations versus spread-spectrum: Chaos and stego security," in *Proc. IIH-MSP*, pp. 208-211, Oct. 2010.

[3] E. Y. Jang and J. Wright, "FPGA implementation of chaos-based digital communication system using CPPM," Dept. of Electronic Engineering Graduate School, Dong-A University, Busan, Korea, Dec. 2007.

[4] G. Kaddoum, P. Charge, D. Roviras, and D. Fournier-Prunaret, "A methodology for bit error rate prediction in chaos-based communication systems," *Springer, Birkhauser Circuits Systems and Signal Processing*, vol. 28, pp. 925-944, 2009.

[5] L. Li and Y. Zhu, "Authentication scheme for substation information security based on chaotic theory," in *Proc. APPEEC 2009*, pp. 1-3, Wuhan, Mar. 2009.

[6] K. Lee, et. al., "The chaotic on-off keying with guard interval for ultra-wideband communication," *IEEE VTS Asia Pacific Wirel. Commun. Symp.*, Daejeon, Korea, Aug. 2006.

[7] N. Abdullah, and A. V. Alejandro, "Performance evaluation of FM-COOK chaotic communication system," *J. Signal Inf. Processing*, vol. 2, pp. 175-177, 2011.

[8] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Trans. Circuits Systems (ISCAS)*, vol. 47, no. 12, Dec. 2000.

[9] M.-I. Jeong, H.-J. Kong, and C.-S. Lee, "Design of transmitter for UWB chaotic-OOK communications," *J. KIEES*, vol. 19, no. 3, pp. 384-390, 2008.

[10] J. Bok and H.-G. Ryu, "Digital chaotic communication system based on CDSK modulation," *J. KICIS*, vol. 38A, no. 6, pp. 479-485, Jun. 2013.

이 준 현 (Jun-Hyun Lee)

2013년 2월 : 충북대학교 전자공학과(공학사)
2013년 3월~현재 : 충북대학교 전자공학과 석사과정
<관심분야> 보안 통신, 이동 통신 시스템

이 동 형 (Dong-Hyung Lee)

1999년 2월 : 충북대학교 전자공학과(공학사)
2001년 2월 : 충북대학교 전자공학과(공학석사)
2001년~현재 : SK Telecom 근무
2007년 3월~현재 : 충북대학교 전자공학과 박사과정
<관심분야> 무선통신 시스템

금 홍 식 (Hong-Sik Keum)

1994년 2월 : 충북대학교 전자공학과(공학석사)
2009년 3월~현재 : 한국전파진흥협회 전자파기술원
<관심분야> 디지털 통신 시스템, EMC, 기술 기준 및 표준화

유 흥 균 (Heung-Gyoon Ryu)

1988년~현재 : 충북대학교 전자공학과 교수

2002년 3월~2004년 2월 : 충북대학교 컴퓨터정보통신연구소 소장

1996년~현재 : IEEE, IET 논문심사위원

2002년 : 한국전자파학회 학술상 수상

2008년 : ICWMC 2008 국제학술대회 “Best Paper Award” 수상

2009년 : SPACOMM 2009 국제학술대회 “Best Paper Award” 수상

<관심분야> 무선 통신 시스템, 위성통신, B4G/5G 이동통신 시스템, 통신회로 설계 및 통신 신호처리