한국통신학회논문지 '13-06 Vol.38A No.06
http://dx.doi.org/10.7840/kics.2013.38A.6.479

CDSK 방식의 디지털 카오스 통신 시스템

복 준 영◆, 유 흥 균°

Digital Chaotic Communication System Based on CDSK Modulation

Junyeong Bok◆, Heung-Gyoon Ryu°

요 약

최근 정보 보안이 중요시됨에 따라서 향상된 보안성과 낮은 도청 확률을 가지는 무선 통신 기술에 대한 관심이 급격히 증가하고 있다. 카오스 신호는 불규칙한 현상으로 인하여 정보를 효율적으로 부호화 하는데 적용할 수 있다. 카오스 신호는 초기 조건에 매우 민감하며 초기 조건을 모른다면 신호의 감지가 어렵다는 단점을 가지고 있지만 다중 경로 간섭에 강한 장점을 가진다. 본 논문에서는 디지털 카오스 변조 방식인 CDSK 방식에서 여러 가지 카오스 맵을 적용하여 수신 성능을 평가한다. 또한, CDSK 방식에서 확산인자 (Spreading factor)의 변화에 따른 수신 BER 성능을 분석한다. 시뮬레이션 결과, Hennon map을 사용할 경우 다른 Chaotic map들 보다 훨씬 좋은 수신 성능을 얻을 수 있었으며, 확산인자가 70에서 가장 좋은 수신 BER 성능을 얻는 것을 확인하였다.

Key Words : Chaotic, CDSK, Henon map, Tent map, Bernoulli shift map.

ABSTRACT

Recently, interest for wireless communication technology with improved security and low eavesdropping probability is increasing rapidly recognizing that information security is an important. Chaos signal can be used encode information efficiently due to irregular phenomena. Chaotic signal is very sensitive to the initial condition. Chaos signal is difficult to detect the signal if you do not know the initial conditions. Also, chaotic signal has robustness to multipath interference. In this paper, we evaluate the performance of correlation delay shift keying (CDSK) modulation with different chaotic map such as Tent map, Logistic map, Henon map, and Bernoulli shift map. Also, we analyze the BER performance depending on the selection of spreading factor (SF) in CDSK. Through the theoretical analyses and simulations, it is confirmed that Henon map has better BER performance than the other three chaotic maps when spreading factor is 70.

Ⅰ. 서 론

오늘날, 향상된 보안성을 통신 시스템에 적용하기 위한 카오스 현상을 이용한 새로운 변조 방식이 큰 관심을 끌고 있다[1-2]. 카오스 신호의 특성은 신호 생성기에서 사용되는 방정식의 초기 조건에 의해서 결정된다. 이렇게 생성된 카오스 신호는 임펄스 형태의 낮은 자기 상관성을 가진다. 낮은 자기 상관성은 초기 조건의 작은 변화에 의해서도 출력은 완전히 다른 형태의 신호로 나타난다. 이러한 특성으로 인해 하나의 카오스 시스템에 다른 초기조건을 적용하여 상호 상관성이 매우 낮은 무한히 많은 카오스 신호를 발생할

※ 본 연구는 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2012017339).
◆ 주저자 : 충북대학교 전자공학과, bjy84@nate.com, 학생회원
° 교신저자 : 충북대학교 전자공학과, ecomm@cbu.ac.kr, 정회원
논문번호 : KICS2013-02-105, 접수일자 : 2013년 2월 26일, 최종논문접수일자 : 2013년 6월 5일

수 있다. 따라서 카오스 통신 시스템은 신호 감청이나 도청이 어려워 보안성을 향상시킬 수 있다[3,4].

카오스 신호는 비주기성과 광대역성을 가진다. 카오스 신호가 가지는 신호의 광대역성과 비주기성으로 인하여, 카오스 신호는 대역 확산 통신 시스템(Spread Spectrum System)에서 사용되는 의사 랜덤 신호(Pseudo random sequency)를 대체 할 수 있다. 카오스 통신 시스템은 확산 코드 대신 카오스 신호를 사용하여 대역 확산을 하므로 보안성이 매우 우수하며, 간섭신호가 포함되어도 역확산 과정에서 확산이 되어 그 크기가 줄어들기 때문에, 외부 간섭에 매우 강한 특성을 가진다. 또한, 전송 신호의 대역폭이 넓기 때문에 페이딩에 강한 특성을 보인다[5,6].

카오스 통신 시스템은 대역 확산코드 대신 카오스 신호를 사용한다[7-9]. 따라서 확산 인자의 선택에 따라서 카오스 통신 시스템의 성능은 변화 하게 된다. 즉 다시 말해 큰 확산 인자를 사용하는 경우에는 대역 효율이 떨어지게 되지만 간섭에 강한 특성을 보인다. 반면에 작은 확산 인자를 사용하는 경우 대역 효율은 증가하나 간섭이나 간섭에 취약하게 된다. 그러므로 채널 환경에 따라서 가장 효율적인 수신 성능을 얻기 위해서는 적절한 확산인자를 선택하는 것이 중요하다.

이러한 카오스 신호의 특성으로 인해 '카오스 이론을 이용한 암호화 기법'이나 '이산화 된 카오스 함수를 이용한 새로운 경량의 암호 시스템', '카오스 암호화 알고리즘을 이용한 보안 시스템 설계 및 구현'과 같은 특정 정보에 대한 암호화 시스템이나 보안 시스템에서도 카오스 신호를 적용시키는 연구가 지속적으로 진행 되고 있습니다.

카오스 통신 시스템은 향상된 보안성과 낮은 도청 확률을 가지며, 초기조건에 매우 민감하여 초기 조건을 모른다면 신호의 감지가 어렵다는 특징을 가진다. 하지만 카오스 통신 시스템은 심볼을 확산인자만큼 카오스 맵 특성에 따라 사상시키고 넓은 범위로 사상하기 때문에 다른 시스템에 비해 BER 성능이 나쁘다는 단점을 가지고 있다.

카오스 통신 시스템은 위에서 서술한 바와 같이 다른 시스템에 비해 많은 장점을 가지지만 BER 성능이 좋지 않다는 단점을 가진다. 본 연구에서는 카오스 맵과 확산인자에 따른 BER 성능을 평가함으로써, 최고의 BER 성능을 가지는 카오스 맵의 종류와 확산 인자를 찾는다. 따라서 이 연구의 결과를 통해 최고의 BER 성능을 갖는 카오스 맵과 확산 인자를 찾아 여러 분야에서 사용되는 카오스 통신 시스템에 적용한다면 단점으로 지적된 BER 성능 열화를 최소화 시킬 수 있다.

본 논문에서는 다양한 카오스 맵에 따른 CDSK 변조 방식의 수신 BER 성능을 분석한다. 또한, 잡음과 간섭이 존재하는 환경에서 확산인자(spreading factor)의 선택에 따라 수신 BER성능을 분석한다. 카오스 맵으로는 Tent map, Logistic map, Henon map, Bernoulli shift map을 이용하였다. 본 논문의 구성은 다음과 같다. 2장에서는 CDSK(correlation delay shift keying) 시스템의 모델을 정의한다. 3장에서는 다양한 카오스 맵에 대해서 설명하고, 4장에서는 성능평가를 위한 시뮬레이션을 진행 한다. 마지막 장에서는 결론을 맺는다.

Ⅱ. 카오스 시스템

본 논문에서 사용된 카오스 통신 시스템의 변조방식은 CDSK 방식이다.

1. CDSK System

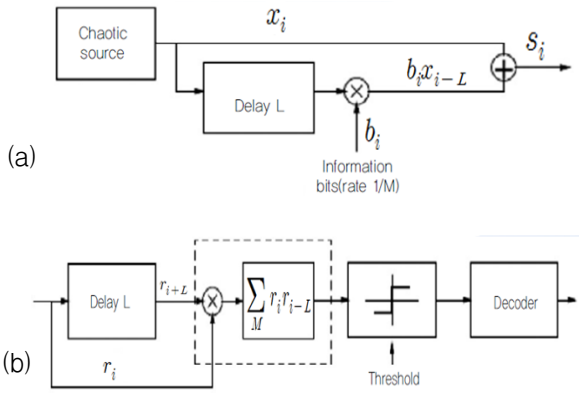


그림 1. CDSK 시스템 블록도
(a) 송신기 (b) 수신기.
Fig. 1. Block diagram of CDSK system
(a)Transmitter (b) Receiver.

그림 1은 카오스 통신 시스템인 CDSK 변조 방식의 시스템 구성도이다. 그림 1.(a)와 같이 CDSK 송신기에서는 카오스 신호 발생기에서 발생된 카오스 신호는 지연된 카오스 신호와 송신 데이터 심볼 곱의 합으로 나타낼 수 있다. 변조된 CDSK 카오스 신호는 식(1)과 같이 표현 할 수 있다.

그림 1(a)는 CDSK 방식의 송신기를 블록도로 나타낸 것이다. 디지털 입력 블록은 전송할 2진 정보 신호를 생성한다. Delay 블록으로 인해 지연이 발생한다. Delay 블록의 출력은 카오스 신호의 플러스 지연 값이며 정보신호와 위의 수식에 따라서 변조된다. CDSK의 상관기 기반 수신기는 심볼을 복구하기 위

해서 사용된다. 따라서 수신기는 식(2)와 같이 수신된 신호와 지연된 신호를 곱하여 정보를 찾을 수 있다.

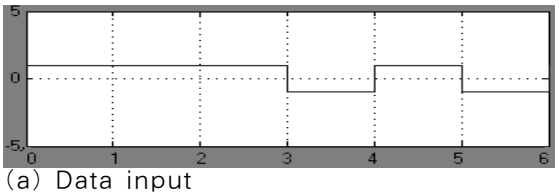
$$S_i = x_i + b_i x_{i-L} \quad (1)$$

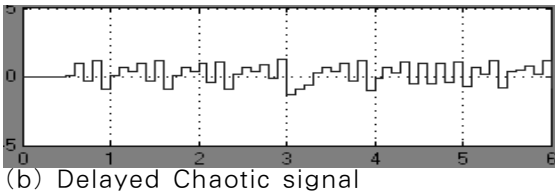
식(1)에서, x_i는 카오스 신호이고, L은 지연된 시간이다. M은 각각의 비트 카오스 신호의 spreading factor이다.

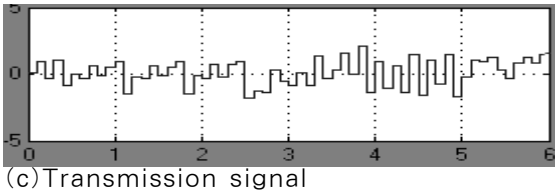
그림 1(b)는 CDSK 방식의 수신기를 블록도로 나타낸 것이다. 디코딩된 심볼은 출력 Y_1이 0보다 크면 “+1”로 결정하고 0보다 작으면 “-1”로 결정한다. CDSK 시스템은 전송신호를 생성하는 스위치가 필요하지 않다. DCSK 시스템의 문제점이었던 송신기에 있는 스위치는 가산기로 대체된다. CDSK는 DCSK가 송신 신호를 반복 전송하는 문제점을 극복한다.

$$Y_1 = \sum_{i=0}^{M} r_i r_{i-L} \quad (2)$$

식(2)에서 M은 확산인자의 길이이고, r_i는 채널을 통과한 수신된 신호이다.


(a) Data input


(b) Delayed Chaotic signal


(c)Transmission signal

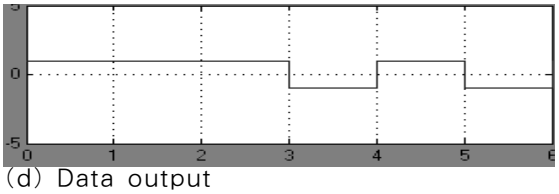
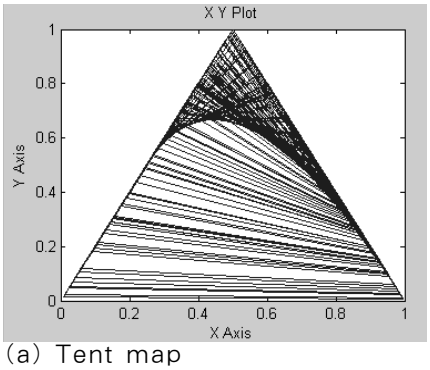

(d) Data output

그림 2. 송수신기의 출력.
Fig. 2. Transceiver output.

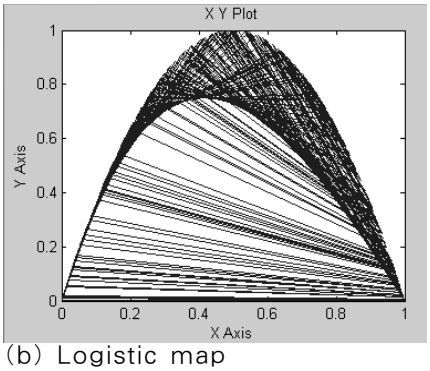
그림 2는 송ㆍ수신기의 출력 신호를 나타낸다. 입력 데이터 신호는 이진 데이터 신호이며, 입력 데이터 신호는 카오스 신호와 곱해진다. 그림 1(a)에서 나타낸 CDSK 송신기처럼 지연된 카오스 신호는 카오스 신호와 더해진 후 전송된다. 전송되는 카오스 신호는 그림 2(c)와 같은 형태를 가진다. 그림 2(d)는 그림 2(c)와 같은 전송된 카오스 신호가 수신기를 거쳐 데이터 신호를 복구한 것을 나타낸다. 그림 2에서는 카오스 맵을 이용한 카오스 통신시스템의 송수신이 가능함을 확인 할 수 있다.

Ⅲ. 카오스 맵

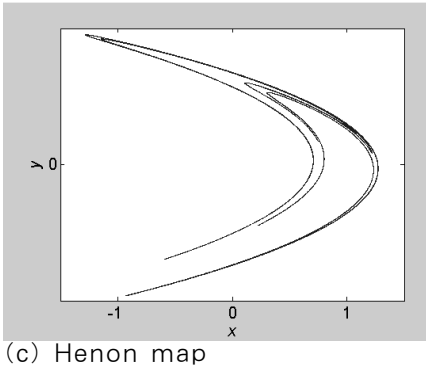
카오스 변조 방식의 성능을 결정 하는 중요한 요인은 카오스 맵이다. 카오스 맵은 카오스 특성을 가진 수식으로 다양한 카오스 맵이 있다. 본 논문에서는 Tent map, Logistic map, Henon map, Bernoulli shift map의 카오스 맵에 대해서 설명한다.



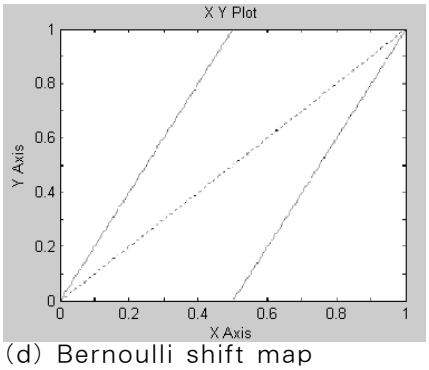
(a) Tent map



(b) Logistic map



(c) Henon map



(d) Bernoulli shift map

그림 3. 다양한 카오스 맵
Fig. 3. Various chaotic map.

그림 3은 위에서 설명한 4가지의 카오스 방정식을 사용한 카오스 맵을 나타낸다.

$$x_{n+1} = \alpha|0.5 - |0.5 - x_n|| \tag{3}$$

Tent map은 현재의 입력으로 이전의 출력 값을 사용하는 비선형 방정식이다. 이득 α의 값이 1.01보다 작을 경우 선형적인 특성을 가지며 α의 값이 증가할수록 출력의 궤적은 더 큰 폭으로 변화하는 특성을 가진다. Tent map 방정식은 식(3) 과 같이 표현되며, 초기 값이 0.1이며 α의 값이 1.9999일 때 그림 3(a)와 같은 궤적을 그린다. 그림 3(a)를 보면 Tent map은 0부터 1까지의 값으로 이루어져 있으며 삼각형 모양을 갖는 것이 특징이다.

$$x_{n+1} = Rx_n(1 - x_n) \tag{4}$$

Logistic map은 수학자 Robert may가 제안한 방정식이다. 이 방정식은 개체는 환경적인 요소에 의해서 독립적으로 증가할 수 없고 보통 포화되거나 발진하기 때문에 선형적인 특성만을 가지지 않는다. Logistic map 방정식은 식(4)과 같이 표현되며, 초기 값이 0.1이며 R 값이 3.9999일 때 그림 3(b)와 같은 궤적을 그린다. 그림 3(b)를 보면 Logistic map은 Tent map과 동일하게 0부터 1까지의 값으로 이루어져 있지만 Tent map과는 다르게 둥근 모양을 갖는 것을 알 수 있다.

$$\begin{aligned} x_{n+1} &= 1 + y_n - a(x_n)^2 \\ y_{n+1} &= bx_n \end{aligned} \tag{5}$$

Henon map 방정식은 가장 연구가 활발히 진행된 카오스 현상을 나타내는 방정식 중의 하나이다. Henon map은 a와 b, 2개의 매개변수에 따라 달라지는데, a=1.4와 b=0.3의 값을 가질 때, 이 방정식을 표준 Henon map 방정식이라고 한다. Henon map 방정식은 식(5)와 같이 표현되며, 표준 Henon map 방정식일 때 그림 3(c)와 같은 궤적을 그린다. 그림 3(c)를 보면 Henon map은 Tent map이나 Logistic map과는 다르게 약 -1.3부터 1.3까지의 값으로 이루어져 있다.

$$\begin{aligned} D(x) &= \begin{cases} 2x & \text{if } 0 \le x < 1/2 \\ 2x-1 & \text{if } 1/2 \le x < 1 \end{cases} \\ &\text{or} \\ D(x) &= 2x \bmod (1) \end{aligned} \tag{6}$$

Bernoulli shift map 방정식은 초기 매개 변수부터 시작하여 매개 변수를 변환시키며, 출력된 매개 변수는 다음 반복의 입력 매개 변수로 사용된다[10]. Bernoulli shift map 방정식은 식(6)과 같이 표현되며 이 방정식으로 그린 궤적은 그림 3(d)와 같다. 그림 3(d)를 보면, Tent map과 Logistic map과 마찬가지로 Bernoulli shift map도 0부터 1까지의 값으로 이루어져 있으며 Bernoulli shift map은 직선으로 표현된다.

Ⅳ. 성능 평가

본 논문에서는 다양한 카오스 맵을 사용한 CDSK 변조 방식의 송수신 성능을 분석한다. 또한, CDSK 변조 방식과 확산 인자의 선택에 따른 수신 성능을 분석한다. 또한, 확산인자의 선택에 따라 BER 성능이 달라짐은 보이고 성능을 최대화 할 수 있는 적절한 확산 인자의 선택조건을 제시한다.

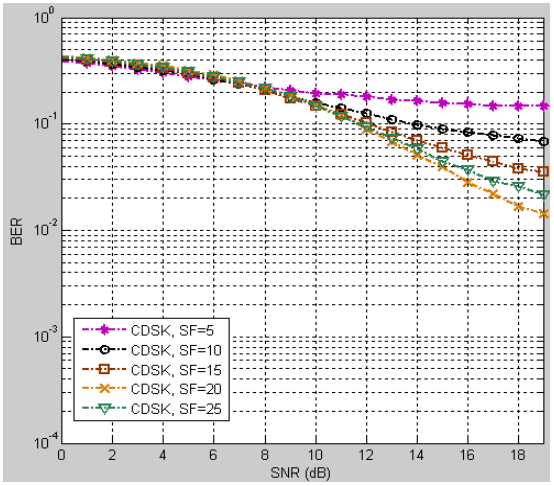


그림 4. Tent map을 사용한 CDSK 시스템의 BER 성능 비교
Fig. 4. BER curves of CDSK system with Tent map.

그림 4는 확산인자의 변화에 따른 Tent map을 사용한 CDSK시스템의 이득변화를 비교한 것이다. Spreading factor가 증가함에 따라서 인접 비트 간섭과 비트 에너지 오류가 감소되는 것을 확인할 수 있다. 큰 확산인자를 사용하는 경우에는 간섭이 줄어들게 되지만, 이득 역시 감소하게 된다. 간섭이 존재하는 환경에서 확산 인자의 선택에 따라 간섭의 영향이 달라진다.

$$BER = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{8N_o}\left(1+\frac{19}{20M}\frac{E_b}{N_o}+\frac{M}{4}\frac{N_o}{E_b}\right)^{-1}}\right) \quad (7)$$

식(7)은 CDSK 방식의 비트 오차율을 식으로 표현한 것이다[3]. 식(7)에서 M은 확산인자를 의미하며, 확산 스펙트럼 통신 시스템은 광대역 주파수에 상대적으로 협대역 정보 신호를 변조시킨다. 그 결과 원하는 신호는 간섭으로 누적되며 채널 잡음과 간섭들은 평균이 된다.

같은 확산인자를 사용할 때 카오스 맵에 따라 BER 성능이 변하는 이유는 식이 변하는 것이 아닌 식의 변수인 E_b와 N_0가 변하기 때문이다. 카오스 맵이 다르면 카오스 신호의 값도 다르다는 의미이며 이 신호의 값이 다르다는 것은 채널잡음이나 인접 심볼간의 에러에 대한 영향을 많이 받는 값으로 변할 수 있는 것을 의미한다. 따라서 카오스 맵이 다르면 E_b와 N_0도 변하게 되며, 이에 따라 BER 성능도 달라지는 것이다.

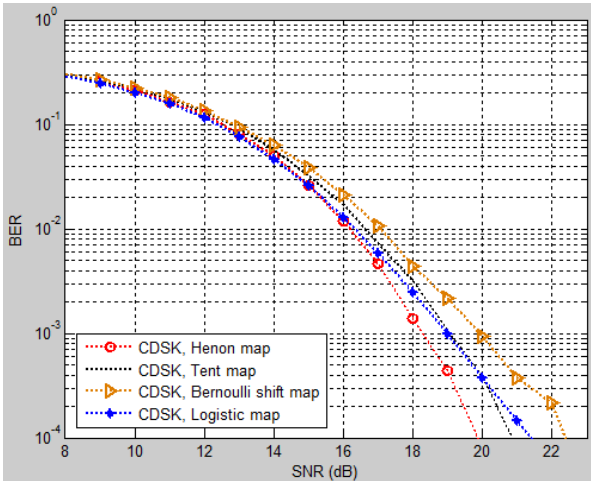


그림 5. Chaotic map에 따른 CDSK 시스템의 BER 성능 비교.
Fig. 5. BER curves of CDSK system with different chaotic maps.

그림 5는 각기 다른 카오스 맵을 사용한 경우에 수신 BER 성능을 분석한 것이다. 그림 5의 결과처럼 Henon map을 사용한 경우가 나머지 다른 세 가지의 맵을 사용했을 경우와 비교해서, 수신 BER 성능이 제일 좋은 것을 확인 할 수 있다. 10^{-4}의 BER에서 Logistic map과 Tent map, Bernoulli shift map의 성능을 비교했을 때, Logistic map과 Tent map은 거의 비슷한 BER 성능을 가지며 Bernoulli shift map보다 약 1dB이상의 좋은 성능을 나타냈으며 Henon map의 경우에는 Logistic map과 Tent map보다 약 1dB이상 더 좋은 성능을 나타낸다. 즉, 그림 5를 통해서 카오스 통신 시스템에서 카오스 맵이 수신 BER 성능에 영향을 미치는 것을 확인 할 수 있다.

그림 5를 보면, 각 카오스 맵마다 BER 성능의 차이가 있다는 것을 알 수 있다. BER 성능 차이가 있는 이유는 CDSK 방식에서 카오스 맵 방정식에 따라서 카오스 신호 생성기에서 출력되는 값이 다르기 때문이다. BER 성능이 나빠지는 요인으로 인접 심볼간의 에러나 수신기에서 임계값을 기준으로 판단할 때 발생하는 에러 등이 있다. 카오스 신호 생성기에서 출력되는 값이 다르다는 것은 BER 성능이 나빠지게 하는 요인에도 영향을 미치며 이로 인해 각 카오스 맵마다 BER 성능의 차이가 있는 것이다.

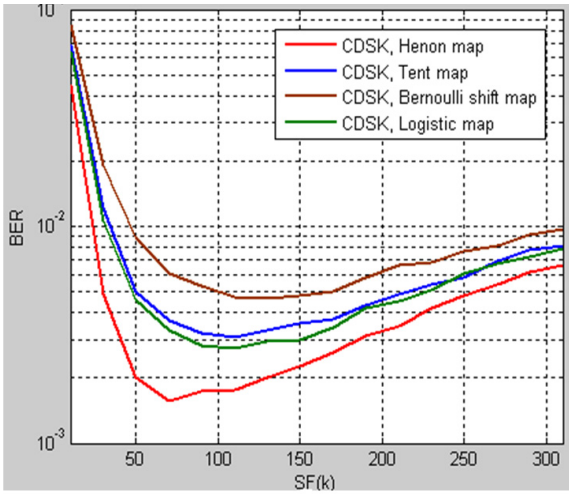


그림 6. 확산인자에 따른 CDSK 시스템의 BER 성능 비교
Fig. 6. BER curves of CDSK system by spreading factor.

그림 6은 서로 다른 확산 인자가 카오스 통신 시스템의 수신 성능에 어떠한 영향을 미치는지에 대한 분석 결과이다. Henon map 의 경우는 확산인자가 70일 경우 수신 BER 성능이 가장 좋은 성능을 보였다. 이에 비해 Logistic map, Tent map, Bernoulli shift map 의 경우 확산인자가 약 100~120에서 가장 좋은 성능을 나타냄을 확인 하였다.

그림 5와 그림 6을 통해서 카오스 맵의 선택에 따라 좋은 BER 성능을 얻을 수 있으며 카오스 맵마다 가장 좋은 BER 성능을 나타내는 확산 인자가 존재하는 것을 알 수 있다. 즉, 적절한 카오스 맵의 선택과 확산인자의 선택을 통해서 향상된 BER 성능을 얻을 수 있는 것이다. 카오스 통신 시스템은 다른 시스템보다 BER 성능이 나쁘기 때문에 향상된 BER 성능을 얻는 것이 굉장히 중요한 과제이다. 따라서 본 논문을 통해 얻은 결과를 토대로 BER 성능을 향상시킬 수 있는 카오스 맵이나 확산 인자를 평가함으로써 카오스 통신 사용자들이 카오스 맵과 확산인자의 적절한 선택으로 향상된 BER 성능을 가질 수 있게 할 수 있다.

V. 결 론

본 논문에서는 카오스 통신 시스템의 한 가지 방식인 CDSK 변조를 사용하는 카오스 통신 시스템의 수신 BER 성능을 여러 가지 카오스 맵의 사용에 따라서 분석하였다. 또한, 확산 인자 (spreading factor)의 선택에 따라서 간섭의 영향과 수신 BER 성능이 어떻게 변화하는지 분석하였다. Spreading factor에 따른 성능 평가에서는 일정한 비트오차율과 Chaotic map을 정하여 동일한 조건에서 성능 평가를 하였으며, 그 결과 Henon map을 사용하였을 때 다른3개의 Chaotic map보다 훨씬 좋은 성능을 내고, SF가 70에서 가장 좋은 성능을 보였다. 따라서 여러 가지의 카오스 맵의 BER 성능을 평가하여 비교하고, 확산인자에 따른 BER 성능을 평가하고 적용함으로써 카오스 통신 사용자들은 향상된 BER 성능을 기대할 수 있다.

References

[1] S. I. Hong and E. Y. Jang, "FPGA implementation of digital transceiver using chaotic signal," *J. Korean Inst. Inform. Technol.*, vol 8. no 8, pp. 9-15, Aug. 2010.

[2] Y. H. Seo and S. M. Kim, "Adaptive data hiding techniques for secure communication of images," *J. Korea Inst. Commun. Inform. Sci.(KCIS)*, vol. 29, no. 5C. pp. 664-672, May 2004.

[3] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.,* vol. 47, no. 12, pp. 1684 - 1691, Dec. 2000.

[4] F. C. M. Lau and C. K. Tse, *Chaos-based digital communication systems*, Springer, 2003.

[5] W. M. Tam and F. C. M. Lau, "Generalized correlation-delay-shift-keying scheme for noncoherent chaos-based communication systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.,* vol. 53, no. 3, pp. 712 - 721, Mar. 2006.

[6] S. Arai and Y. Nishio, "Variable sequence length transmitter for noncoherent chaos shift keying," in *Proc. RISP Int. Workshop Nonlinear Circuits Signal Process. (NCSP'06)*, pp. 301-304, Honolulu, U.S.A., Mar. 2006.

[7] S. Arai and Y. Nishio, "Noncoherent correlation-based communication systems choosing different chaotic maps," *IEEE Int. Symp. Circuits Syst. (ISCAS 2007)*, pp. 1433 - 1436, New Orleans, U.S.A., May 2007.

[8] T. J. Wren and T.-C. Yang, “Orthogonal chaotic vector shift keying in digital communications,” *IET Commun.*, vol. 4, no. 6, pp. 739 - 753, Apr. 2010.

[9] H. Yang and G.-P. Jiang, “High-efficiency differential-chaos-shift-keying scheme for chaos-based noncoherent communication,” *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 59, no. 5, pp. 312-316, Apr. 2012.

복 준 영 (Junyeong Bok)

2010년 2월 충북대학교 전자공학과(공학사)

2012년 2월 충북대학교 전자공학과(공학석사)

2012년 3월~현재 충북대학교 전자공학과 박사과정

<관심분야> 무선 통신 시스템, 이동 통신 시스템

유 흥 균 (Heung-Gyoon Ryu)

1988년~현재 충북대학교 전자공학과 교수

2002년 3월~2004년 2월 충북대학교 컴퓨터정보통신연구소 소장

1996년~현재 IEEE, IET 논문 심사위원

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 이동 통신 시스템, 통신회로 설계 및 통신 신호 처리