비동기 카오스 비밀통신의 변복조 기술평가

최희주* · 배준호* · 김성곤* · 변건식*

*동아대학교

Comparative Evaluation of Modem Technique in Nonsynchronous Chaos Secure Communication

Hee-Joo Choi* · Joon-Ho Bae* · Sung-Gon Kim* · Kun-Sik Byon*

*Donga University

E-mail:ksbyon@mail.donga.ac.kr

요 약

1994년 이래, 광대역 통신 시스템에 카오스 이론을 적용하는 연구가 지속되어 왔으며 지금까지 여러가지 변복조기술이 개발되어 왔다. 변복조기술은 두 종류로 나눌 수 있다. 첫째는 동기 복조 기술로, 동기에 의해 카오스 신호를 수신 신호로부터 재생하는 것이다. 그러나 카오스 동기 기술은 채널 잡음이나 왜곡에 매우 민감하며 이 기술은 무선 통신에 사용되기 힘들다. 둘째는 비동기로 복조를 하는 것이다. 본 논문은 비동기로 구현할 수 있는 여러가지 카오스 통신 기술을 설명하고 임계값과 오율등을 비교 평가한다. 특히 비동기 FM-DCSK는 판정회로에 필요한 임계값이 잡음레벨에 상관없이 0으로 임계값 선정이 쉽고 데이터율이 카오스 신호의 성질에 의해 제한되지 않음을 입증함으로서 앞으로 비동기 FM-DCSK가 카오스 디지털 CDMA 시스템의 기반기술로 응용될 수 있음을 확인하였다.

ABSTRACT

During the past five years, there has been tremendous interest worldwide in the possibility of exploiting chaos in wideband communication systems. Many different demodulation techniques have been proposed up to date. They can be divided into two basic categories. In the first approach, like the conventional coherent demodulation techniques, the chaotic signal has to be recovered from the received noisy signal by synchronization. However, the chaotic synchronization techniques published to data are so sensitive to the channel noise and distortion that these techniques can not be used in radio communications. In the second approach, the demodulation is carried out nonsynchronization. This paper surveys the different chaotic communication techniques that can be implemented nonsynchronization and compares the threshold and BER of the different methods. Finally, FM-DCSK is introduced the first step for apply to wideband chaos digital CDMA, where the data is not limited by the inherent nonperiodic property of the chaotic signal.

Ⅰ. 서 론

이동 통신 시스템, 무선 LAN, 면허가 필요없는 무선 통신등은, 음성과 데이터 전송 서비스가 필요하다. 전통적인 협대역 통신 시스템은 이러한 응용분야에서 많은 단점을 갖는다. 즉, 협대역 신호는 다중로 전파에 의해 생긴 선택성 페이딩에 민감하며, 높은 송신 전력은 다른 사용자에게 심한 간섭을 일으킨다. 이와같은 협대역 시스템은 스펙트럼 확산통신을 이용하면 개선할 수 있다. 스펙트럼 확산통신은 전송 대역폭을 광대역으로 만드는 기술이며 또 다른 광대역 발생으로는 전송 심볼을 비주기 카오스 신호로 나타내는 것이다. 카오스 신호는 광대역 전력 스펙트럼으로 특성화 되며 시간영역에서는 그림1과 같이 랜덤하게 나타난다.

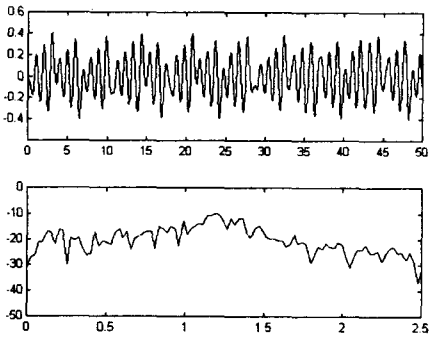


그림 1. 시간영역과 주파수영역의 카오스신호

카오스 신호는 초기조건에 매우 민감하며, 작은 동요는 시스템 상태에 큰 변화를 발생한다. 카오스 신호의 자기상관 함수는 0에서 큰 피크를 가지며 빠르게 감소한다. 즉 카오스 신호는 통계적 프로세스의 성질을 가지지만 결정적 구조도 갖고 있다. 카오스 신호의 중요한 성질은 매우 간단한 회로로 발생할 수 있는 비주기적 광대역 신호라는 것이다. 따라서 연속시간 카오스 시스템은, 카오스를 기반으로하는 카오스 디지털 CDMA을 하기 위한 광대역 캐리어를 만드는데 사용될 수 있다. 카오스 CDMA시스템에서, 전송할 정보는 카오스 파형으로 사상되며 전송 심볼은 동기 및 비동기 복조로 재생할 수 있다. 잡음성 수신신호에서 정보전송을 수행하는 파라미터를 추정하면 재생이 가능하므로 비동기 복조를 사용할 수 있다. 카오스 함수의 파라미터는, 카오스 신호가 비주기적이기 때문에 변화한다. 주기신호를 사용하는 전통적인 통신시스템과는 달리, 카오스 신호의 판정에 필요한 파라미터는 잡음이 없을 때 조차도 추정해야 한다. 추정시 분산은 채널 잡음과 카오스 신호에 의해 영향을 받는다. 잡음 크기가 주어질 때, 추정시 분산은 추정시간(비트폭)을 늘임으로서 줄일수 있다. 비트폭은 주어진 SNR로 이루어야하는 BER에 의해 제한된다. 제1세대 비동기 카오스 변복조기술인 CSK(chaos shift keying)의 단점은 판정회로에 필요한 임계값이 SNR에 의존한다는 것이다[1]. 이를 개선하기 위해 다음의 COOK(chaos on-off keying)변복조 방식을 사용한다.

II. COOK

가장 좋은 잡음 성능은, 잡음 레벨과 카오스 신호가 주어졌을 때, 두 개의 평균값 사이의 거리를 최대로 하면 얻을 수 있다. 비트에너지 E_b가 주어질때, 2진 신호의 원소사이의 최대 거리는 COOK기술로 해결가능하며, COOK에서 카오스 신호는 그림2와 같이 심볼 0과 1에 의해 스위칭된다.

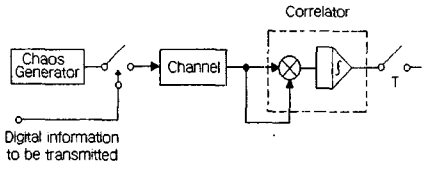


그림 2. 비동기 COOK 시스템

이 경우, 신호 집합의 원소사이의 거리는 E_b 이다. 그림3은 잡음이 없는 경우의 히스토그램이다. 만약 송신신호가 통신 채널에서 잡음을 수반하면, 히스토그램은 그림4와 같이 된다. 여기서 판정을 위한 최적 임계값은 점선으로 주어진다. 그림5는 비동기 COOK의 잡음 성능이다. 여기서 파라미터는 심볼폭이다. 똑같은 BER에 대해, COOK는 CSK에 비해서 E_b/N_0가 8dB 낮다[4]. T_b는 비트당 샘플수이다. COOK가 잡음 성능이 더 좋은 것은, 신호 집합 원소 사이의 거리가 CSK에 비해서 증가했다는 사실 때문이다. 그러나, CSK의 주된 단점인 판정회로의 임계값이 잡음 레벨에 영향을 받는것이 COOK에도 역시 나타난다. 이 의미는, COOK를 사용해서 신호 집합 원소 사이의 거리를 최대화할 수 있지만, 판정회로에 필요한 임계값은 SNR에 의존한다는 의미이다.

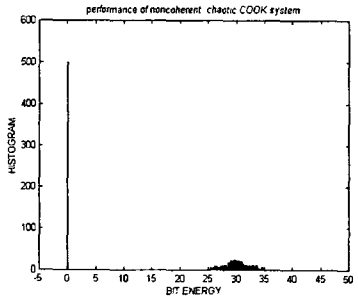


그림 3. 잡음 없이 비동기 COOK 시스템에 수신된 신호의 히스토그램

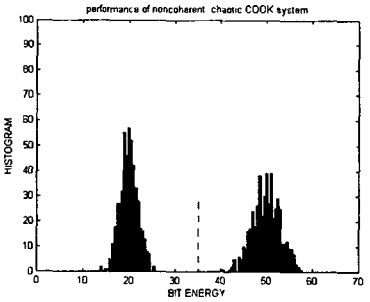


그림 4. 비동기 COOK 수신기에 잡음이 수신된 신호의 히스토그램

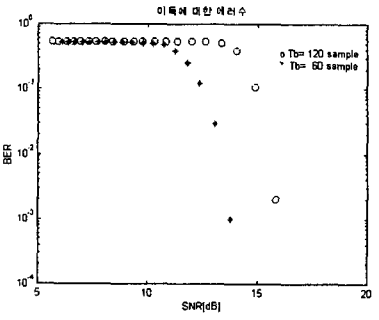
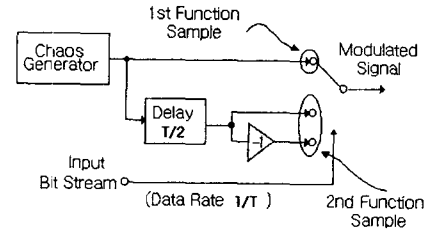


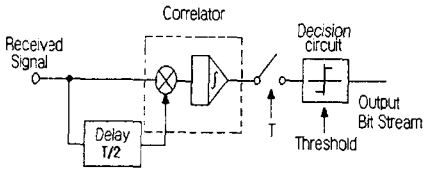
그림 5. 비동기 COOK시스템의 잡음성능

III. DCSK

임계값이 SNR에 의존하는 COOK의 단점을 제거한 비동기 DCSK(differential CSK) 송수신기는 그림6과 같다.



(a)송신기



(b)수신기

그림 6. DCSK 시스템의 블럭도

DCSK에서 전송할 모든 비트는, 두 개의 카오스 샘플 함수로 표시된다. 첫 번째 샘플 함수는 표준 함수로 동작하며, 두 번째 함수는 정보를 전송한다. 비트 1은 두 번 연속 카오스 발생기에서 공급된 표준 신호에 의해서 전송되며, 식(1)과 같다[2].

$$x_{transmitted} = \begin{cases} x(t), & t_k \le t < t_k + T/2 \\ x(t - T/2), & t_k + T/2 \le t < t_k + T \end{cases} \quad (1)$$

비트 0은 처음에 표준 카오스 신호가 전송되고 그 다음 그 신호의 반전신호가 전송되며 식(2)와 같다.

$$x_{transmitted} = \begin{cases} x(t), & t_k \le t < t_k + T/2 \\ -x(t - T/2), & t_k + T/2 \le t < t_k + T \end{cases} \quad (2)$$

이 의미는 2진 정보가 두부분의 송신 신호 사이에서 측정한 상관으로 사상된다. 결국 한비트의 다음 반주기의 상관값으로 2진정보를 판정한다. 수신된 잡음성 신호는 비트폭의 절반 만큼 지연되며, 수신 신호와 지연된 신호사이의 상관이 구해진다. 판정은 레벨 비교기로 행해진다. 잡음 없는 DCSK에서, 판정 시간에서의 상관기 출력은 비트당 에너지의 절반이다. 이 의미는 DCSK에서, 신호 원소사이의 거리는, COOK에서 처럼 E_b 와 같다는 의미이다. 채널 잡음이 없을 때, 상관기 출력신호의 히스토그램은 그림7과 같다.

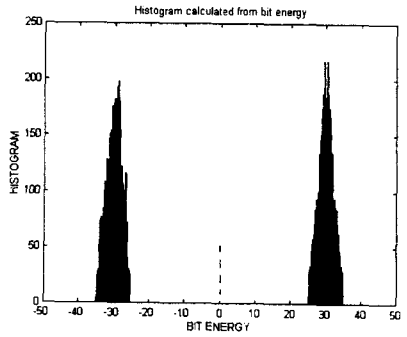


그림 7. 잡음이 없이 DCSK시스템에 수신된 신호의 히스토그램

이 그림에서 임계값은 E_b/N_0와는 독립으로 0임을 보여준다. CSK나 COOK와 같은 카오스 변조에 대해 DCSK의 주된 장점은 DCSK는 대척 변조 기술을 사용한다는 것이다. 즉 DCSK는 신호원소 사이에 거리를 최대로 한다. 결과적으로 잡음 성능이 우수하며 기존의 정현파를 기본으로 하는 통신 시스템과 비교 할 수 있다. DCSK 수신기의 판정회로에 필요한 임계치는 무선채널에서 측정한 SNR과 상관 없이 항상 0이다. DCSK 변조법은 BER=10E-3에 대하여 E_b/N_0=13.3dB가 필요하다[4].

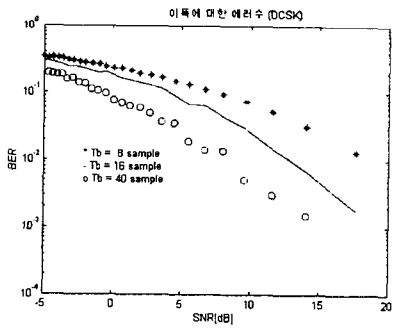


그림 8. DCSK 시스템의 잡음성능

전송할 정보 신호는 DCSK변조 기술에서 유한 길이의 카오스 샘플에 사상된다. 카오스 신호의 비 주기적 성질 때문에, 상관 즉 비트당 에너지는 같은 심볼이 연속적으로 송신 되더라도 심볼에서 심볼로 변한다. 이 의미는 수신기가 비록 잡음이 없더라도 정보를 전송하는 상관만을 추정할 수 있다는 의미이다. 그림7은 이 문제를 설명하며, 판정 회로 입력에서의 히스토그램이 무잡음인 경우를 도시하였다. 이 추정은 0이 아닌 분산을 가지기 때문에 잡음성능이 좋지 않다.

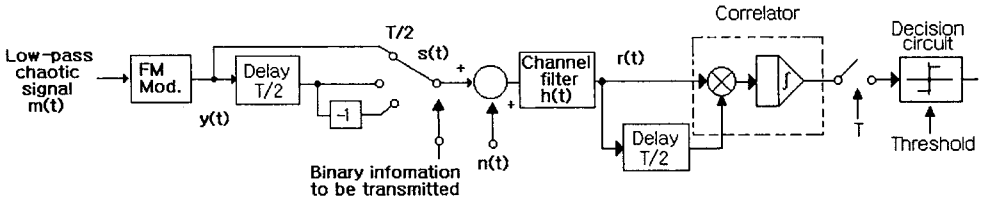


그림 9. FM-DCSK 시스템의 블럭도

추정의 분산이 클수록, 수신기에서 부정확한 판정을 하는데 필요한 부가 채널 잡음의 크기는 작아진다. 따라서 추정의 분산을 최소화해야 한다. 히스토그램의 분산은 추정시간 즉 비트폭(sample 수)을 증가함으로써 줄일 수 있다. 그러나 추정시간이 클수록 데이터율은 작아지며 데이터율은 제한된다[3,4]. 추정문제는 FM과 DCSK기술을 조합하면 DCSK의 우수한 잡음성능을 희생하지 않고 극복 할 수 있다.

IV. FM-DCSK

일정한 E_b를 갖는 광대역 신호를 발생하는 것이 필요하다. FM 신호의 순시 전력은 변조에 의존하지 않는다[5]. FM신호기의 입력을 카오스 신호라 하자. FM변조기의 광대역 출력이 DCSK를 사용해서 변조되면, 수신기의 상관기 출력은 잡음이 없는 경우, 분산을 가지지 않는다. DCSK에서처럼, 모든 정보 비트는 두 개의 샘플 함수에 의해 전송된다. 첫 번째 부분은 표준 신호이고, 두 번째 부분이 정보를 전송한다. 변조기의 동작은 DCSK와 같으며 단지 차이는 DCSK변조기의 입력이 카오스가 아니라 FM변조된 신호라는 것이다. 비트 1은 두 번 연속 카오스신호에 따른 FM 발생기에서 공급된 표준FM신호에 의해서 전송된다. 식(3)은 카오스신호에 따른 FM신호이고 식(4)는 FM-DCSK신호이다.

$$y(t) = A_c \cos 2\pi\left\{f_c t + k_f \int_0^t m(\tau)d\tau\right\} \qquad (3)$$

$$y_{transmitted} = \begin{cases} y(t), & t_k \le t < t_k + T/2 \\ y(t - T/2), & t_k + T/2 \le t < t_k + T \end{cases} \qquad (4)$$

비트 0은 처음에 표준 FM신호가 전송되고 그 다음 그 신호의 반전신호가 전송되며, 식(5)와 같다.

$$y_{transmitted} = \begin{cases} y(t), & t_k \le t < t_k + T/2 \\ -y(t - T/2), & t_k + T/2 \le t < t_k + T \end{cases} \qquad (5)$$

그림9와 같이, FM변조기의 입력은 카오스 신호이다. 만약 저주파 카오스 신호가 만들어 진다면, FM변조기의 출력은 균일 전력 밀도를 갖는 대역 제한된 스펙트럼을 갖는다는 것을 알 수 있다. FM-DCSK의 복조기는 DCSK수신기와 같으며 단지 차이는 저주파 카오스 신호 대신에, FM신호가 곧바로 상관된다는 것이다.

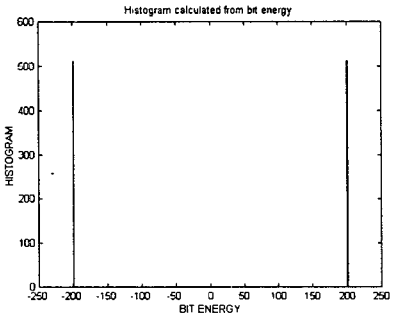


그림 10. 잡음이 없이 FM-DCSK 수신기에 수신된 신호의 히스토그램

그림10은 잡음이 없는 경우의 히스토그램이다. FM-DCSK변조에 의해 추정의 분산은 0임을 알 수 있다. 그림11은 잡음이 있을 때의 히스토그램이다.

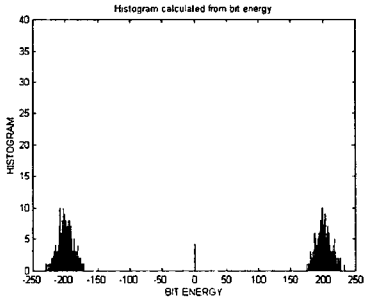


그림 11. FM-DCSK 수신기에 잡음이 수신된 신호의 히스토그램

판정회로에 필요한 임계 레벨은 잡음 레벨에 상관 없이 항상 0임에 주목하라. 그림12는 FM-DCSK 시스템의 잡음 성능이다. 앞에서 제시한 다른 디지털 카오스 변조 기술에 대한 FM-DCSK변조의 장점은, 데이터 율이 카오스 신호의 성질에 의해 제한되지 않는다는 것이다.

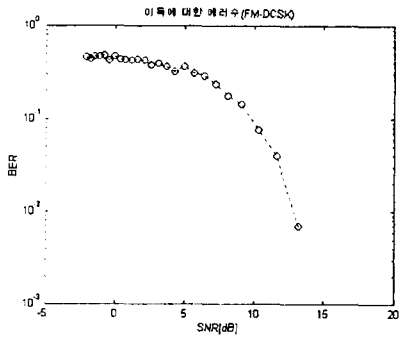


그림 12. FM-DCSK의 잡음 성능

V.결론

비동기 카오스 변복조 기술인 COOK, DCSK, FM-DCSK를 비교 분석하였다. 카오스 신호의 비주기 성질에 의해, 비트 에너지는, 잡음이 없는 경우에서 조차 DCSK 수신기에서만 추정할 수 있다. 만약 규정된 잡음 성능을 얻기 위하여, 임의 한계 이하로 관찰 신호의 분산값을 유지하려면, 충분히 큰 비트폭을 선택해야한다. 데이터율은 비트폭에 의해 구해지기 때문에, 추정 문제는 데이터율이 카오스 캐리어 신호의 통계적 문제에 의해 제한 받는다는 의미이다. 이 문제는 FM-DCSK로 극복할 수 있으며 FM과 DCSK변조 기술이 추정 문제를 해결하기 위하여 조합된다.

FM-DCSK복조기에서, FM변조된 고주파 신호는 전송된 디지털 정보를 재생하기 위해 곧바로 상관된다. FM-DCSK에서 비트 에너지는 카오스 신호에 종속되지 않는다. 즉, 추정의 분산은 잡음이 없는 경우 0이다. 다시말해 데이터율이 시스템에 사용된 카오스 신호의 성질에 의해 제한받지 않는다는 것이다.

FM-DCSK는 앞으로 카오스 디지털 CDMA시스템 구현의 초석이 될것으로 생각되며 지속적으로 연구할 계획이다.

참고문헌

[1] Kennedy M P and Dedieu H, 1993, "Experimental demonstration of binary chaos shift keying using self-synchronizing Chua's circuits", In Proc. on NDES, 67-72

[2] Kolumbn G, Vizvari B, Schwarz W, and Abel A, 1996, "Differential chaos shift keying: A robust coding for chaotic communication", In Proc. on NDES, 87-92

[3] Kolumbn G, Kennedy M P and Kis G, 1997, "Determination of symbol duration in chaos-based communications", In Proc. on NDES, 217-222

[4] Kolumbn G, Dedieu H, Schweizer J, Ennitis J, and Vizvari B, 1996, "Performance evaluation and comparison of chaos communication systems", In Proc. on NDES, 105-110

[5] Roden, 1996, "Analog and Digital Communication Systems", Prentice Hall, Fourth edition.