

본 논문은 잘 알려진 혼돈 지도를 기반으로 생성한 이진 혼돈 수열 및 위성 항법 신호의 PRN 부호인 Kasami 부호를 NIST 통계적 테스트인 NIST SP 800-22를 통해 비주기·비예측적 군통신에 대한 특성을 적합성을 검증한다.

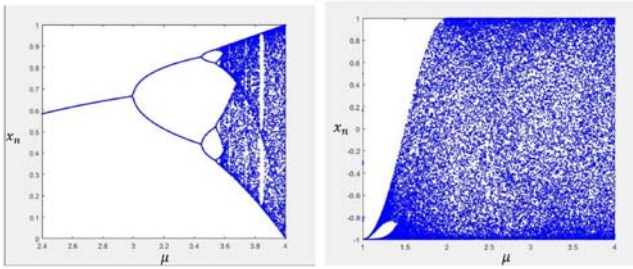
■ 개요

R. L. Devaney가 정의한 동적 시스템의 혼돈(chaos) 개념은 비선형 동적 시스템에서 비주기적, 무질서 상태를 말하며, 혼돈 신호는 비선형 동적 시스템에 의해 생성되는 비주기적 의사 난수 신호로, 현재 상태에서 다음 상태를 결정하는 규칙에 의해 고유하게 결정될 수 있다[1].

위성 항법 시스템은 중심 주파수가 공개되어 있어 공격에 취약하다. 그러므로 혼돈 신호의 특성을 활용하여 jamming/spoofing, 다중 경로 환경에 대한 보상, 그리고 다양한 유형의 잡음에 대한 강건성을 향상시키기 위한 연구가 진행되고 있다[2-3].

본 논문은 기존 혼돈 지도를 이용하여, 이진 혼돈 수열을 생성 및 기존 위성 항법 시스템에 사용되는 PRN 부호와 함께 NIST 통계적 테스트를 통해 강건성에 대하여 분석을 보인다.

• 혼돈 지도(Chaotic map)



(a) Logistic map

(b) Chebyshev map

비선형 동적 시스템에 의해 생성된 혼돈 신호는 비주기적이고 유사 무작위 특성을 가진다. 비선형 동적 시스템은 현재 상태 x_n 를 기반으로 다음 상태 x_{n+1} 를 고유하게 결정하는 일련의 규칙과 함께 모든 가능한 상태 집합 V 로 구성된다.

(a) Logistic map

- $x_{n+1} = \mu \cdot x_n(1 - x_n)$
- $1 \leq \mu \leq 4, x_n \in (0,1)$
- when $\mu \in [3.5699, 4]$, the map is chaotic

(b) Chebyshev map

- $x_{n+1} = \cos(\mu \cdot \cos^{-1}(x_n))$
- $0 \leq \mu \leq 4, x_n \in [-1,1]$
- when $\mu \geq 2$, the map is chaotic

(c) Chen's map

- $\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz - cy \\ \dot{z} = xy - bz \end{cases}$
- when $a = 35, b = 3, c = 28$, the map is chaotic

• NIST STATISTICAL TEST

NIST SP 800-22는 테스트 가설을 기반으로 시퀀스가 무작위인지 여부를 결정하는 일련의 통계 테스트다. 귀무가설은 주어진 수열이 임의적이라는 것이며, 귀무가설을 수용/기각 결정을 위해 무작위성 통계가 사용된다. P -값은 귀무가설에 대한 증거의 강도를 요약한 것이며, P -값이 0.01보다 크면 테스트가 99% 신뢰도로 만족된다는 것을 의미한다[7]. 본 논문은 15개의 테스트 중 적절한 6개에 대해 분석한다.

(1) Frequency (Monobits)

1과 0의 수가 무작위 수열에서 예상되는 것과 거의 같은 지 확인

(2) Run

다양한 길이의 1과 0의 'Run' 횟수가 임의 시퀀스에 대해 예상한 것과 같은 지 확인

(3) Rank

수열 내 특정 길이의 부분 수열 간의 선형 종속성을 확인

(4) DFT

테스트된 수열에서 임의성 가정에서 벗어난 주기적인 특징 (즉, 서로 가까이 있는 반복 패턴)을 감지

(5) Linear Complexity

수열이 무작위로 간주될 만큼 충분히 복잡한지 여부를 결정

(6) Cumulative Sum (Cusum)

수열 내 부분 수열의 누적 합계가 예상하는 무작위 수열에 대한 누적 합계의 예상 동작에 비해 너무 크거나 작은 지 여부를 결정

• 테스트 결과 및 결론

표 1. 이진 혼돈 수열의 초기값

Map	Initial values	Threshold
Logistic	$\mu = 4, x_0 = 0.4$	$\theta = 0.5$
Chebyshev	$\mu = 4, x_0 = 0.4$	$\theta = 0.0$
Chen	$x_0 = -3, y_0 = 2, z_0 = 20$	-

표 2. NIST 통계적 테스트 결과 (P -값)

Test	Classification			
	Logistic	Chebyshev	Chen	Kasami
Frequency	0.5341	0.7399	0.3504	0.3504
Runs	0.0668	0.9114	0.0043	0.3504
Rank	0.3504	0.1223	0.3504	0.0000
DFT	0.3504	0.7399	0.5341	0.0000
Linear Complexity	0.0351	0.3504	0.5341	0.0000
Cusum (forward)	0.3504	0.7399	0.3504	0.0179

본 논문에서는 표 1과 같은 초기값으로 혼돈 수열을 생성하고, 임계값 θ 를 기준으로 생성된 수열을 이진화하여 이진 혼돈 수열을 생성한다. 테스트에 필요한 비트스트림의 수는 10개로 설정하고, 비트스트림의 길이는 10230개(QZSS LEX의 PRN 코드 길이와 동일)로 설정한다[8]. 테스트 관련된 파라미터는 NIST 800-22의 초기값과 동일하게 적용하였다.

표 2는 위에서 설명한 혼돈 지도 의해 생성된 이진 혼돈 수열과 QZSS LEX에서 사용된 Kasami 부호의 NIST SP 800-22 결과를 보여준다. Kasami 코드의 경우 Rank, DFT 및 Linear Complexity 테스트에 임의성이 적절하지 않다. 이는 단순 LFSR로 생성된 Kasami 부호의 특성으로 보인다. Chen 지도의 경우 Runs 테스트 대한 임의성이 적절하지 않음을 보여준다. 추후 이진화에서 적절한 임계값을 선택하기 위한 분석이 필요하다.

ACKNOWLEDGMENT

이 (성과)는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.RS-2023-00209000).