

## 다양한 재밍 환경에서 시간도약 시스템 성능 분석

정효영<sup>\*,1)</sup> · 이종환<sup>2)</sup> · 김기선<sup>1)</sup>

<sup>1)</sup> 광주과학기술원국 전기전자컴퓨터공학

<sup>2)</sup> 국방과학연구소 제2기술연구본부

### On the Performance of Time-Hopping Systems under Hostile Jamming Environments

Hyoyoung Jung<sup>\*,1)</sup> · Jong-Hwan Lee<sup>2)</sup> · Kiseon Kim<sup>1)</sup>

<sup>1)</sup> School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, KOREA

<sup>2)</sup> The 2nd Research and Development Institute, Agency for Defense Development, Korea

(Received 19 May 2017 / Revised 13 September 2017 / Accepted 8 December 2017)

#### ABSTRACT

In this paper, we consider the applicability of time-hopping(TH) systems for anti-jamming(AJ) communication. We first briefly summarize fundamentals of TH systems and several common jamming scenarios that have been considered in the literature. We then analyze the AJ performance of TH systems under those common jamming environments. From our simulation results, we reveal that among narrow band, partial band, broadband, and sweep jamming, partial band and sweep jamming are the best ones from jammer perspective. For the partial band jamming case, we show that the most effective bandwidth ratio and location are 50 % and 2.5-3.5 Ghz, respectively. For the sweep jamming case, we illustrate that the AJ performance of the TH system is enhanced when the sweep duration approaches to the bit duration. In addition, we pointed out that the most efficient jamming bandwidth ratio is 1/2. Finally, our results show that the TH-BPSK system greatly outperforms the TH-PPM counterpart.

Key Words : Time-Hopping(시간도약), Spread Spectrum(대역확산), Anti-Jamming(항재밍), Partial Band Noise Jamming(부분대역재밍), Sweep Jamming(스위프재밍)

#### 기 호 설 명

$T_c$  : 칩 시간 (s)

$T_s$  : 프레임 시간 (s)

$E_b N_0$  : 신호 대 잡음비 (dB)

SJR : 신호 대 재밍비 (dB)

$\rho$  : 실효 재밍 대역폭 비율

\* Corresponding author, E-mail: rain@gist.ac.kr

Copyright © The Korea Institute of Military Science and Technology

BER : 비트 에러 레이트

## 1. 서론

현대 통신의 개방성으로 인해 무선통신은 다른 신호들의 간섭, 의도된 제밍 공격들에 쉽게 방해받는다. 따라서 제밍 공격은 더 이상 군통신에 국한되지 않고 민간 및 상용 통신에서도 중요한 과제가 되었다. 제머는 공격하고자 하는 통신시스템의 주파수 대역에 제밍 신호를 전송한다. 효과적인 제밍 공격이 이루어지기 위해 목표 시스템의 전송기와 수신기의 위치를 파악하고 수신부를 향해 신호를 전송해야만 한다. 제밍 공격 주 목적은 정보의 질을 낮추고 정보전달을 지연 시킴으로써 전장 환경에서 적군의 통신을 방해하는 것이다. 그 결과 학계와 산업 모두에서 강력한 항제밍 시스템을 설계하는 연구가 활발히 진행되어 왔다.

대역확산(Spread Spectrum, SS) 시스템은 제밍공격에 대비한 항제밍 시스템으로 전술 군사 시스템에서 개발되었지만 그 효율성 때문에 이동통신, 위성통신, 그리고 근거리 통신 분야에서 활발히 활용되고 있다. 가장 대표적인 SS 기법으로 주파수도약(Frequency Hopping, FH)과 직접 시퀀스(Direct Sequence, DS) SS 시스템이 존재한다. FHSS 시스템은 pseudorandom sequence를 이용해서 보내고자 하는 신호의 carrier 주파수를 바꾸어 간다. 반면 DSSS 시스템은 매우 낮은 파워 밀도를 넓은 주파수 대역에 펼쳐 보냄으로써 신호의 검출과 공격을 어렵게 하는 기법이다. 최근에는 FHSS와 DSSS의 항제밍 성능을 개선하기 위해 hybrid FH-DS SS 시스템이 제안되었다<sup>[1,2]</sup>.

비록 DS와 FH 시스템이 많이 활용되고 있지만 몇 가지 단점들이 있다. DSSS 시스템은 Gold sequence와 같은 유사잡음 sequence를 채택함으로써 다중접속 성능 감소한다. FHSS 시스템은 구현이 복잡하고 팔로우 제머(follow jammer)와 신호를 변장하거나 속이는 스마트 제밍환경에서 성능을 보장해 주지 못한다. 이러한 DSSS와 FHSS 시스템의 단점을 보완하기 위해 강건하고 효율적인 SS 시스템이 필요하다. 그 하나의 가능성으로 시간도약(Time Hopping, TH)시스템이 존재한다. TH 시스템은 sub-nanosecond의 파형(monocycle)을 임의로 지연시킴으로써 carrierless 전송과 더불어 SS 특성을 지니게 된다. TH 시스템은 FHSS와 DSSS보다 구현이 간편하다<sup>[3]</sup>. 게다가 TH 시스템은 적절한 TH

sequence(THS)를 이용해서 다중접속 환경에 활용할 수 있다<sup>[4]</sup>. 하지만 다른 SS 시스템과는 달리 TH 시스템을 항제밍 시스템 측면에서 성능 검증한 연구가 불충분한 상황이다. 따라서 본 논문에서는 TH 시스템 모델, 특성, 그리고 종류에 대해서 정리한다. 또한 다양한 제밍 시나리오에 대해 설명하고 해당 제밍에서 항제밍 성능을 검증한다. 성능검증 시뮬레이션에서는 제밍의 효과와 파라미터들이 TH 시스템에 미치는 영향을 보여준다.

본 논문의 구성은 다음과 같다. TH 시스템 모델, 특성, 그리고 종류를 Section II에서 소개한다. Section III에서는 고려하고 있는 다양한 제밍 환경에 대해서 서술한다. Section III에서 다른 제밍에 대해서 Section IV에서 항제밍 성능 시뮬레이션 수행하고 Section V에서 결론에 대해 서술한다.

## 2. TH 시스템

### 2.1 TH 시스템 모델

TH 시스템에서 전송되는 파형을 모노사이클(monocycle)이라고 부르고 1 ns 미만의 전송시간을 갖는다. 이러한 전송비트는 보내는 THS 코드에 따라 전송 시점 즉 칩 슬롯으로 분배되고 모노사이클 파형으로 성형하여 최종적으로 전송된다. 이러한 전송신호는 낮은 파워 밀도와 넓은 대역폭을 갖는다.

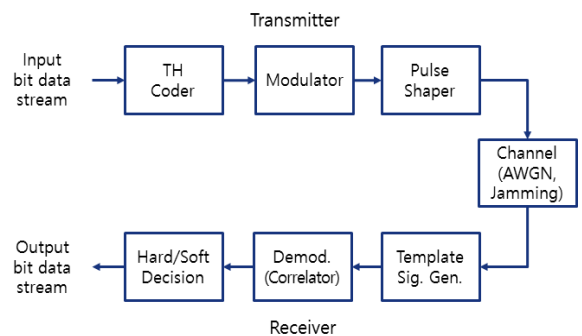


Fig. 1. TH system block diagram

Fig. 1은 TH 시스템의 구조도를 나타낸다. 처음으로 정보 비트 스트림은 각 비트들이  $N_b$ 번 반복된다. TH coder에서는  $N_h$ 의 cardinality와  $N_p$ 의 주기를 갖는 THS를 생성하고 이에 따라 반복된 정보 스트림의 각 비

트정보들을 지정된 시간위치인 칩 슬롯에 위치시킨다. THS는 각 수가  $0,1,\dots,N_h$ 의 값을 갖는  $N_p$  개의 랜덤 숫자 수열이다. 한 비트의 프레임 시간  $T_s$ 은 칩시간  $T_c$ 을 갖는  $N_h$ 개의 칩으로 구성된다. 변조기에서는 TH coded 된 비트를 BPSK 또는 PPM의 기법에 따라 변조한다. 마지막으로, pulse shaper에서는 모노사이클을 생성하고 최종적으로 변조된 정보에 실어 전송하는 신호를 생성하게 된다. 본 논문에서의 수신채널은 다양한 재밍공격과 수신부에서 발생하는 additive white Gaussian noise(AWGN)가 중첩된 채널을 가정한다.

수신된 신호는  $r(t) = s(t) + j(t) + n(t)$ 로 나타낼 수 있다. 수신부에서의 template signal generator에서는 모노사이클을 고려하여 복조에 사용하는 레퍼런스신호  $v_w(t)$ 를 다음과 같이 생성한다.

$$v_w(t) = w(t; b_k = 0) - w(t; b_k = 1),$$

여기서  $w(t)$ 는 모노사이클 그리고  $b_k$ 은  $k$ 번째 비트를 의미한다. 복조기에서는 TH code  $\{c_m\}$ 를 기준으로 동기화된 레퍼런스신호  $v_w(t)$ 와 수신 신호  $r(t)$ 의 상관관계 값  $R_k$ 을 다음과 같이 계산한다.

$$R_k = \sum_{m=kN_s}^{kN_s+N_s-1} \int_{mT_j+kT_b}^{(m+1)T_j+kT_b} [r(t) \cdot v_w(t - mT_f - c_mT_c)] dt$$

Decision 블록에서는  $R_k$ 가 0보다 크면 비트 “0”으로 0보다 작으면 비트 “1”로 분류한다. TH 시스템의 bit error rate(BER) 성능은 에러가 발생한 비트수를 전송한 총 비트수로 나누어 계산한다.

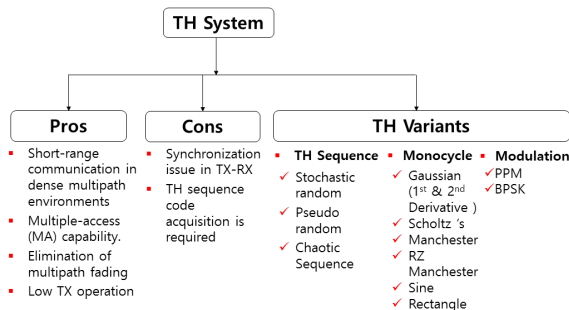


Fig. 2. Characteristics and variations of TH system

## 2.2 TH 시스템 특성

TH 시스템은 정보전달에 주기가 짧은 파형을 사용하기 때문에 구현이 용이한 carrierless 통신이 가능하다. 또한 TH 시스템은 넓은 대역대를 사용함으로써 기존의 통신시스템에 간섭이 적은 다중접속 통신을 가능케 한다. 게다가 TH 시스템 다중 경로 환경에서 페이딩 효과를 대폭 줄여준다. 하지만 전송부와 수신부의 동기화 과정에서 복잡도가 매우 높고, 수신부가 TH code 정보를 얻어야 한다는 어려움이 있다.

## 2.3 TH System Variants

TH 시스템은 THS, 모노사이클, 그리고 변조 방식에 따라 여러 종류로 구분할 수 있다. THS는 신호를 보낼 칩 슬롯을 결정하는 임의의 수열이다. THS의 종류로는 stochastic, pseudorandom, 그리고 chaotic 수열이 존재한다. Stochastic THS는 가장 이론적인 랜덤 수열이지만 구현하기에 매우 복잡하여 실현가능성이 적다. Pseudorandom THS는 간단하고 구현이 용이하지만 랜덤성이 적어 다중접속 통신에서 충돌이 발생할 가능성이 존재한다. Chaotic THS는 위 장단점들을 종합해 보았을 때, 가장 실용적인 THS라고 할 수 있다. Logistic, tent, 그리고 bernoulli 맵과 같은 다양한 chaotic 맵이 존재하고, 좋은 상관관계 특성을 지닌다.

TH 시스템에서 실제 정보 비트를 전송하게 되는 파형인 모노사이클은 BER과 다중경로 특성에 영향을 준다. 모노사이클 종류에는 Gaussian, Sholtz, Manchester, Return-to-Zero(RZ) Manchester, sine, 그리고 rectangular 모노사이클이 존재한다. Gaussian 모노사이클은 Gaussian 파형을 일차 미분한 것을 나타낸다. Scholtz's 모노사이클은 Gaussian pulse를 2차 미분한 형태를 갖는 파형이다. Manchester 모노사이클은 반주기동안 A의 크기를 나머지 반주기동안 -A의 크기를 갖는 파형이다. RZ Manchester 모노사이클은 Manchester 모노사이클에서 크기를 갖는 주기가 반으로 줄인 파형이다. Sine 모노사이클은 간단한 한주기 삼각함수 파형이고, rectangular 모노사이클은 전 주기 동안 A의 크기를 갖는 구모양의 파형이다. 본 논문에서는 Scholtz's 모노사이클을 고려한다. Scholtz's 모노사이클은 다른 파형들 보다 넓은 대역폭을 지니며 다중경로 특성이 우수하다고 알려져 있다<sup>[5]</sup>. 수학적으로 Scholtz's 모노사이클은 다음과 같이 표현된다.

$$w(t) = A \left[ 1 - 4\pi \left( \frac{t - T_c}{T_{au}} \right)^2 \right] \exp \left[ -2\pi \left( \frac{t - T_c}{T_{au}} \right)^2 \right],$$

여기서  $A$ 는 신호의 크기  $T_{au}$  파형 성형 파라미터이다.

TH 시스템은 변조 방식에 따라 TH-PPM 그리고 TH-BPSK로 구분된다. TH-PPM에서는 정보 비트가 “0”이면 일반적으로 모노사이클은 전송하고, “1”이면 칩 슬롯에 모노사이클을 시간 지연( $\delta$ )만큼 지연시켜 전송함으로써 정보 비트를 변조한다. TH-PPM의 전송 신호  $s_{PPM}(t)$ 는 다음과 같다.

$$s_{PPM}(t) = \sum_{j=-\infty}^{\infty} w_{tr}(t - jT_f - c_jT_c - \delta d_{\lfloor j/N_s \rfloor}),$$

여기서  $w_{tr}$ 은 TH 시스템의 모노사이클,  $c_j$ 는 TH code이다. TH-BPSK에서 정보 비트 “1”은 +1 그리고 “0”은 -1의 부호변화로 정보를 변조한다. TH-BPSK의 전송 신호  $s_{BPSK}(t)$ 는 다음과 같다.

$$s_{BPSK}(t) = \sum_{j=-\infty}^{\infty} (2d_{\lfloor j/N_s \rfloor} - 1) w_{tr}(t - jT_f - c_jT_c)$$

### 3. 재밍 공격 시나리오

잡음재밍공격은 잡음 신호를 적의 송수신부에 전송하는 대전자전 전자공격의 한 종류이다. 잡음재밍은 적 장비에 대한 사전지식을 많이 요구하지 않기 때문에 실전에서 효율적으로 쓰이는 기법이다. 본 논문에서는 TH 시스템의 항재밍 성능을 검증하기 위해 전대역 잡음재밍(Broad Band Noise Jamming, BBNJ), 협대역 잡음재밍(Narrow Band Noise Jamming, NBNJ), 부분대역 잡음재밍(Partial Band Noise Jamming, PBNJ), 그리고 스위프 재밍(Sweep Jamming, SJ)을 고려한다. Fig. 3과 Fig. 4에서는 본 논문에서 고려하는 재밍들의 주파수 스펙트럼을 보여준다.

#### 3.1 전대역 잡음재밍(BBNJ)

전대역 잡음재밍은 목표 시스템의 전대역에 균일한 파워 밀도의 잡음 신호를 보내어 방해하는 재밍 공격이다. 주요한 특징으로 넓은 대역 범위를 공격할 수 있다는 장점이 있지만 그만큼 파워 밀도가 전대역으로 퍼진다는 단점을 동반한다.

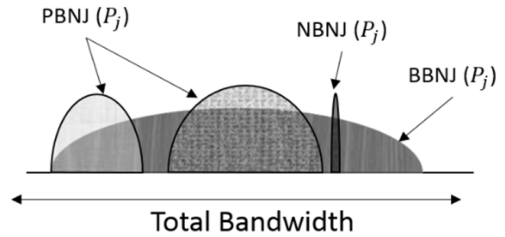


Fig. 3. Noise jamming scenarios: BBNJ, NBNJ, and PBNJ

#### 3.2 협대역 잡음재밍(NBNJ)

협대역 잡음재밍은 좁은 주파수 대역에 재밍 파워를 집중해서 공격하는 기법이다. 협대역 잡음재밍은 상황에 따라 전체 대역 중 원하는 주파수 대역에 공격을 집중할 수 있다는 장점이 있다. 톤 재밍은 협대역 잡음재밍의 한 종류로  $f_j$ 의 한 특정 주파수에 집중해서 공격하는 재밍 기법이다.

#### 3.3 부분대역 잡음재밍(PBNJ)

부분대역 잡음재밍은 전체 대역폭의 한 부분에 재밍 파워를 집중하여 공격하는 재밍이다. 부분대역 잡음재밍은 주파수 하한  $B_l$ 과 주파수 상한  $B_u$ 로 특징지어진다. 부분대역 잡음재밍에서 재밍이 가해지는 주파수 대역은 실제 시스템에 공격이 부분적으로만 가해질 수 있기 때문에, 실효재밍비율( $\rho$ )을 정의해야만 한다. 실효재밍비율( $\rho$ )은 전체 목표 대역폭 대비 실제 공격이 가해지는 실효 대역폭으로 정의된다.

$$\rho = \frac{W_j}{W_{TH}},$$

여기서  $W_j$ 는 부분대역 잡음재밍이 실제 시스템 대역폭 안에서 가해지는 대역폭 크기를 의미하고,  $W_{TH}$ 은 TH 전송 신호의 전체 대역폭 크기를 의미한다.

#### 3.4 스위프 재밍(SJ)

스위프재밍(SJ)은 특정  $0 \sim T_{SJ}$  시간 동안 스위프 파형의 주파수를 주파수 하한  $B_l$ 부터 주파수 상한  $B_u$ 까지 변화해가며 재밍하는 공격이다. 현대 복잡한 SS기법들이 신호의 주파수 정보를 숨기거나 또는 재밍 공격을 회피하여 기존의 재밍 공격을 무력화한다. SJ은 이러한 항재밍 시스템을 짧은 시간 안에 신호

전대역을 집중된 에너지로 이동하면서 재밍 함으로써 재밍 성공률을 높이는데 효과적이다<sup>[7]</sup>. Fig. 4에서 SJ와 TH 신호의 시간-주파수 스펙트럼을 나타낸다.

비록, 스위프 파형, 스위프 가속 종류, 스위프 가속 방향, 스위프 가속 패턴으로 여러 가지 SJ이 존재하지만, unidirectional positive linear single tone(UPLST) SJ이 가장 대표적이다. Unidirectional positive linear 스위프 주파수는  $0 \leq t \leq T_{SJ}$ 의 시간동안  $f_{SJ}(t) = B_l + \frac{B_u - B_l}{T_{SJ}}t$ 와 같이 선형적으로 주파수를 증가 시키는 함수로 표현된다. 또한 single tone은 일반적으로 한 정현파 함수  $\cos \psi_{SJ}(t)$ 로 나타내어진다. 여기서 주파수함수  $f_{SJ}(t)$ 는 위상함수  $\psi_{SJ}(t)$ 의 미분 함수이기 때문에, 즉  $f_{SJ}(t) = d\psi_{SJ}(t)/dt = B_l + \frac{B_u - B_l}{T_{SJ}}t$ , 위상함수는  $\psi_{SJ}(t) = B_l t + \frac{B_u - B_l}{2T_{SJ}}t^2$ 과 같이 구할 수 있다. 따라서 UPLST SJ의 수식은 다음과 같고 Fig. 4와 같은 스펙트럼을 지닌다.

$$j_{SJ}(t) = \sqrt{P_f/2} \cos 2\pi \psi_{SJ}(t)$$

$$= \sqrt{P_f/2} \cos 2\pi \left( B_l t + \frac{B_u - B_l}{2T_{SJ}} t^2 \right) \quad \forall t \sim [0, T_{SJ}]$$

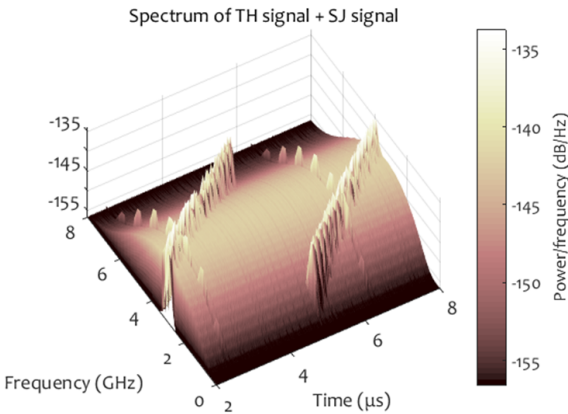


Fig. 4. Time-frequency spectrum of SJ and TH signal

#### 4. TH 시스템의 항재밍 성능

이 장에서는 3장에서 설명한 재밍 시나리오 환경 하에 TH 시스템의 항재밍 성능을 분석한다. 본 논문

에서 고려하는 TH 시스템에서는 싱글 유저를 가정하고 전송 채널은 잡음재밍 공격과 AWGN 잡음을 가정한다. 재밍공격을 고려한 수신 신호는 다음과 같다.

$$r(t) = s_i(t) + n(t) + j(t),$$

여기서  $r(t)$ 는 수신된 TH 신호,  $s_i(t)$ 는 전송된 TH 신호이며,  $i$ 는 변조방식에 따라 PPM 또는 BPSK로 Section II.3에서 주어진다.  $n(t)$ 는 AWGN 신호이고,  $j(t)$  채널 중 인가된 재밍신호이다. Table 1은 본 시뮬레이션에 사용된 파라미터들을 나타낸다. 본 장에서 모든 재밍 환경에서 가장 TH 시스템에 치명적인 재밍을 보이고 가장 위협적인 PBNJ와 SJ환경에서 주요 파라미터들이 항재밍 성능에 미치는 영향을 분석한다. 마지막으로 SJ환경에서 TH-PPM과 TH-BPSK의 성능을 비교한다.

Table 1. Simulation parameter

Parameter	Value
Number of bits	$10^4$
Chip time ( $T_{cf}$ )	1 ns
Number of pulse per bit ( $N_p$ )	3
Cardinality of TH code ( $N_h$ )	4
Period of TH code ( $N_p$ )	100
Frame time ( $T_s$ )	$N_h * 1$ ns
Pulse shaping factor ( $\tau$ )	0.25 ns
Pulse duration ( $T_m$ )	0.5 ns
PPM time shift ( $\delta$ )	0.5 ns
Monocycle	Scholtz's
Simulation sampling time	0.02 ns
Eb/No	15 dB

##### 4.1 대역확산 기법들 비교

Fig. 5에서는 전대역 잡음재밍 환경 하에 TH-PPM 시스템, DSSS 시스템, 그리고 FHSS 시스템의 SJ대비 BER 성능을 Eb/No값이 10 dB와 15 dB인 환경에서 시뮬레이션 하였다. 실험에 사용한 FHSS시스템과 DSSS 시스템은 [7]에서 사용되었다. FHSS시스템과 DSSS시

시스템의 chip 개수는 TH-PPM과 같이 3개를 가정하였다. FHSS시스템과 DSSS시스템의 BER성능 그래프는 노란색 그리고 빨간색으로 나타나며, [7]에서 유도한 이론값이다. 시뮬레이션 결과에서 TH-PPM 시스템의 저 SJR과 고SJR 모두에서 항재밍 성능이 FHSS와 DSSS 시스템보다 강인하다는 것을 확인할 수 있다. FHSS 시스템은 저 SJR일 때 대략 -10 dB이하의 SJR 구간에서 가장 열악한 항재밍 성능을 나타내며, -5 dB 이상의 SJR 구간에서는 TH-PPM 시스템과 동등한 항재밍 성능을 보여준다. 실험 결과 TH-PPM 시스템이 BBNJ 환경에서 항재밍 시스템으로 다른 대역확산시스템보다 유용하다는 것을 보여준다.

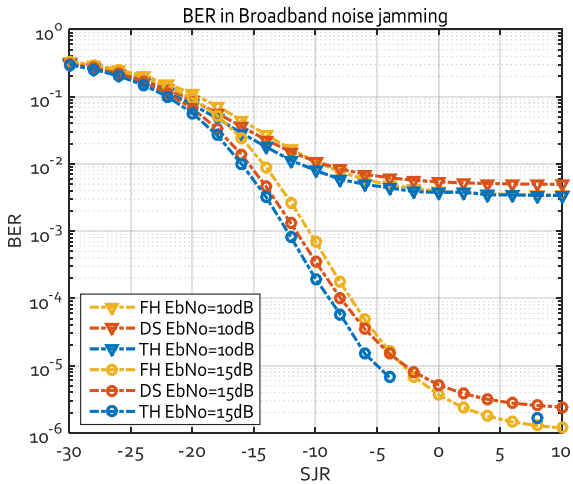


Fig. 5. BER under several jamming scenarios for the TH system, the DS system, and the FH system

#### 4.2 모든 재밍 시나리오 비교

Fig. 6에서는 모든 재밍 환경 하에 TH-PPM의 SJR 대비 BER 성능을 시뮬레이션 하였다. Table 1의 파라미터들을 시뮬레이션 하였을 때 TH-PPM 시스템의 99%의 에너지는 1 GHz부터 6 GHz의 주파수대역대에 분포한다. 목표 대역폭을 5 GHz(1 GHz ~ 6 GHz)이고  $E_b N_0 = 15$  dB인 환경에서, NBNJ의 재밍 주파수  $f_j$ 는 2.2 GHz, PBNJ와 SJ의 주파수 하한  $B_l$ 은 1 GHz, 주파수 상한  $B_u$ 는 3.5 GHz, 그리고 스위프 주기는 16 ns로 설정하였다. 그림에서 SJ가 재밍관점에서 가장 강력하다는 것을 확인할 수 있고, PBNJ는 SJ와 유사한 재밍 성능을 보여준다. 따라서 다음 절에서는 PBNJ와 SJ 중점적으로 TH 시스템의 항재밍 성능을 분석한다.

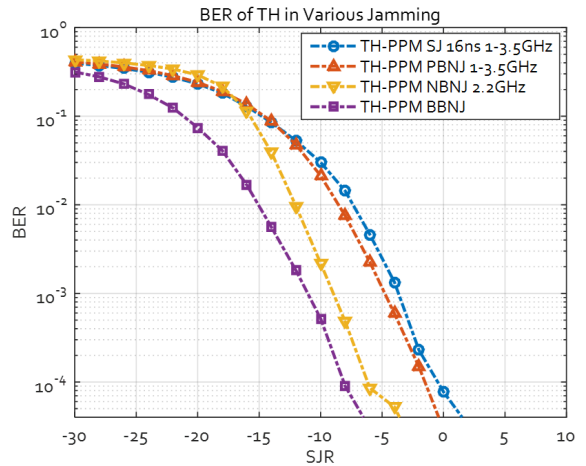


Fig. 6. BER of the TH-PPM system under several jamming scenarios

#### 4.3 부분대역 잡음재밍

Fig. 7은 실효재밍비율이 10%와 30%일 때 PBNJ 환경에서 다른 주파수 위치에 따른 TH-PPM의 항재밍 성능을 나타낸다. 일정한 재밍비율 즉  $B_u - B_l$ 을 유지 하면서  $B_l$ 을 1 GHz에서 5.5 GHz까지 0.5 GHz 간격으로 변화시킨다. 파란 그래프는 비율이 10% 즉  $B_u - B_l = 0.5$  GHz, 그리고 빨간 그래프는 비율이 30% 즉  $B_u - B_l = 1.5$  GHz 일 때 그래프이다. 10%의 재밍비율일 경우 2.5 GHz와 3 GHz에서 30%의 재밍비율일 경우 2 GHz와 2.5 GHz일 때 TH-PPM의 BER성능이 가장 저하되는 것을 확인할 수 있다. 실제 재밍 공격되어지는 영역을 알아보면 PBNJ가 2.5 ~ 3.5 GHz를 공통적으로 공격할 때, 재밍성능은 가장 강력해지고 가장 많은 에러를 발생시킴을 확인할 수 있다. TH-PPM 시스템 관점에서 분석하면 2.5 ~ 3.5 GHz 대역이 가장 취약한 대역폭이라는 점을 알 수 있다.

Fig. 8은 PBNJ 환경에서  $E_b N_0 = 15$  dB, SJR = -5, -10, -15 dB,  $B_l = 1$  GHz, 그리고  $B_u = 1.5$  GHz ~ 6 GHz으로 0.5 GHz 간격으로 증가시킬 때 TH-PPM의 항재밍 성능을 보여준다. SJR이 -5과 -10 dB 일 때, 재밍비율이 10%에서 30%에서는 성능변화가 미비하고, 30%에서 50% 증가 할 때 TH-PPM 시스템 성능도 급격히 감소한다. 또한 50%를 초과한 비율에서는 포화한다. SJR값이 -15 dB일 때는 재밍비율에 따르는 성능격차가 -5와 -10 dB 일때에 비해 크지 않다. SJR이 -5, -10, 그리고 -15 dB일 때, TH 시스템의 BER 값

은 각각  $10^{-3}$ , 0.02, 그리고 0.1로 수렴한다. 따라서, 이 실험을 통해 항재밍 성능의 포화를 고려한 PBNJ 환경에서 가장 효율적인 재밍비율은 50 %임을 알 수 있다.

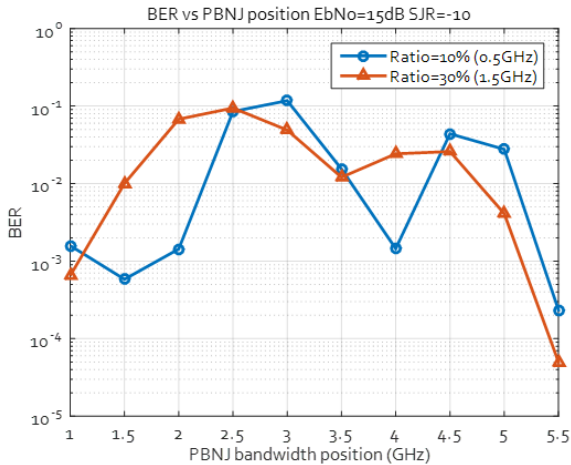


Fig. 7. BER of the TH-PPM system versus PBNJ position when  $E_b/N_0 = 15$  dB and  $SJR = -10$  dB

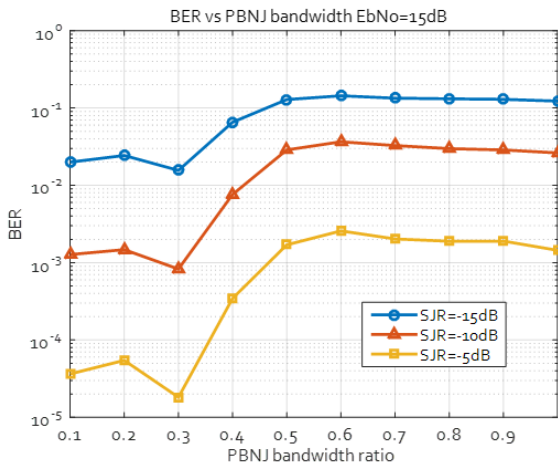


Fig. 8. BER of the TH-PPM system versus PBNJ bandwidth when  $E_b/N_0 = 15$  dB and  $SJR = -5, -10, \text{ and } -15$  dB

#### 4.4 스위프 재밍

Fig. 9는 UPLST SJ환경에서 주파수 하한  $B_l = 1$  GHz이고 주파수 상한  $B_u = 6$  GHz 일 때 스위프 주

기에 따른 TH-PPM 시스템의 항재밍 성능을 보여준다. TH 시스템의 구조로 계산하면 하나의 비트를 전송하기 위해  $T_{bit} = N_h T_c N_s$ 의 시간이 필요하다. Fig. 8로부터 SJ의 스위프 주기  $T_{SJ}$ 가  $T_{bit} = 12$  ns와 유사해 질 때 TH-PPM 시스템의 BER 성능이 가장 우수하다. 이는 재밍 성능 관점에서 보면 성능저하를 의미하고, 스위프 주기  $T_{SJ}$ 가  $T_{bit}$ 에서 멀어질 때 재밍 성능은 더 강화된다는 것을 알 수 있다.

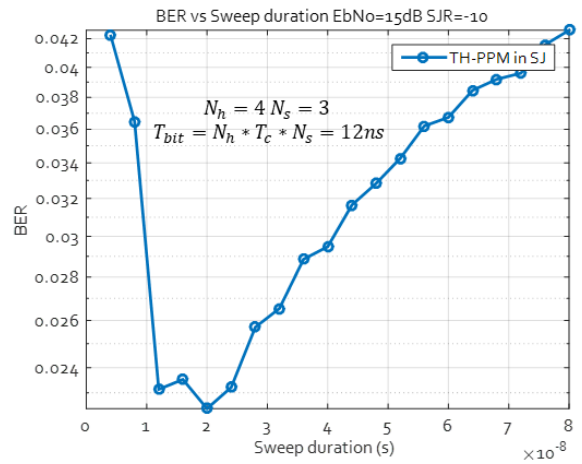


Fig. 9. BER of the TH-PPM system versus sweep duration when  $E_b/N_0 = 15$  dB and  $SJR = -10$  dB

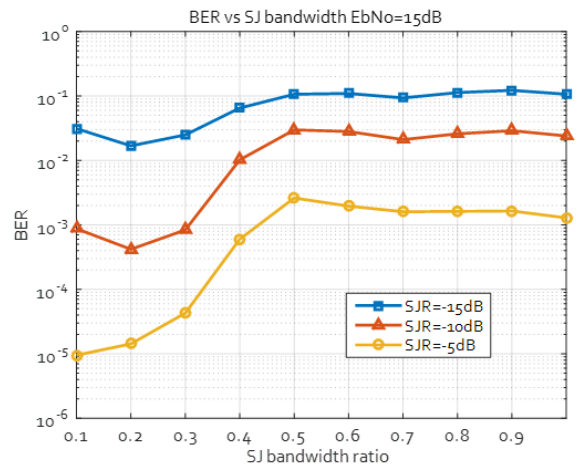


Fig. 10. BER of the TH-PPM system versus bandwidth ratio when  $E_b/N_0 = 15$  dB and  $SJR = -5, -10, \text{ and } -15$  dB

Fig. 10에서는 UPLST SJ 실효재밍비율에 따른 TH-PPM 시스템의 항재밍 성능을 보여준다. 실험은  $E_bN_0 = 15$  dB 잡음채널 환경에서 SJR이 -5, -10, 그리고 -15 dB인 세 가지 재밍환경에 대하여 BER을 보여준다. 주파수 하한  $B_l = 1$  GHz,  $T_{SJ}$ 는 Fig. 9에서 관찰한 최적의 시간 16 ns로 고정하고,  $B_u$ 을 1.5 GHz부터 6 GHz까지 0.5 GHz 간격으로 증가시키며 시뮬레이션 하였다. 결과는 Fig. 8의 PBNJ 환경에서의 결과와 일치한다. 재밍비율이 30 %에서 50 % 증가할 때 BER 성능이 저하되고, 50 % 이상의 재밍비율에서 BER 성능은 포화된다. SJR 값이 감소함에 따라 재밍비율에 의해 발생하는 BER 성능격차가 줄어든다. PBNJ환경과 유사하게 SJ환경에서 50 %의 재밍비율 즉 1 GHz ~ 3.5 GHz의 재밍 대역폭이 가장 효과적인 것을 확인하였다.

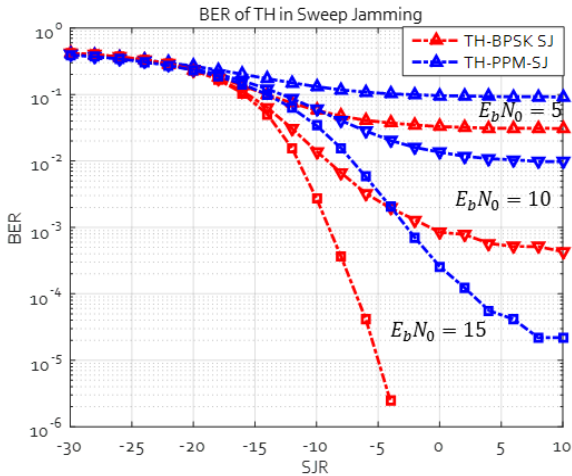


Fig. 11. BER of the TH-PPM and the TH-BPSK systems under SJ when  $E_bN_0 = 15$  dB and  $SJR = -10$  dB

Fig. 11에서는 UPLST SJ환경에서 재밍공격을 방어하기에 더 적합한 시스템을 확인하기 위해 TH-PPM과 TH-BPSK의 SJR대비 항재밍 성능을 비교하였다. 본 시뮬레이션에서는  $E_bN_0 = 5, 10$ , 그리고 15 dB 일 때 항재밍 성능을 비교하였다. 파란 그래프는 TH-PPM 그리고 빨간 그래프는 TH-BPSK의 BER성능을 의미한다. 결과로 TH-BPSK가 TH-PPM보다 항재밍 성능이 우수하다는 것을 알 수 있고, 그 격차는  $E_bN_0$  값이 커질수록 커진다. 이러한 항재밍 성능 개선은 TH-PPM은 orthogonal signaling을 사용하고 TH-BPSK는 antipodal

signaling을 사용하는데서 찾을 수 있다. Antipodal 신호가 orthogonal 신호보다 파워를 더 효율적으로 쓰기 때문에 항재밍 성능이 좋아진다는 것을 확인할 수 있다.

## 5. Conclusion

본 논문에서는 전대역, 협대역, 부분대역 잡음재밍, 그리고 스위프 재밍 환경에서 TH-PPM과 TH-BPSK를 포함하는 TH 시스템의 항재밍 성능을 검증하였다. 앞서 언급한 재밍 공격 중 PBNJ와 SJ 재밍이 가장 위협적인 것을 확인하였다. PBNJ의 경우 50 %의 실효재밍비율일 때 최적으로 시스템 성능을 저하시키고, 2.5 GHz ~ 3.5 GHz 대역의 TH 신호를 공격할 때 TH 시스템의 성능이 급격히 저하되는 것을 확인하였다. 또한 SJ의 경우 스위프 주기에 따라 TH 시스템의 항재밍 성능이 달라지고 스위프 주기가 비트 한 개를 보내는 시간과 유사해 질 때 항재밍 성능이 강화된다는 것을 확인하였다. 게다가, 재밍관점에서 SJ재밍의 가장 효과적인 실효재밍비율은 50 %이었다. 마지막으로 TH-BPSK가 TH-PPM보다 월등히 좋은 항재밍 성능을 갖는다는 것을 확인하였다.

## 후 기

The authors gratefully acknowledge the support from Electronic Warfare Research Center at Gwangju Institute of Science and Technology(GIST), originally funded by Defense Acquisition Program Administration(DAPA) and Agency for Defense Development(ADD).

## References

- [1] Kanika Grover, Alvin Lim, Qing Yang, "Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey," *Int. J. Ad Hoc Ubiquitous Comput.*, 17 (4), pp. 197-215, 2014.
- [2] Y. Liu, P. Ning, H. Dai and A. Liu, "Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication," 2010 Proceedings IEEE INFOCOM, San Diego, CA, pp. 1-9, 2010.



- [3] M. Z. Win, "A Unified Spectral Analysis of Generalized Time-Hopping Spread-Spectrum Signals in the Presence Of Timing Jitter," in IEEE Journal on Selected Areas in Communications, Vol. 20, No. 9, pp. 1664-1676, Dec. 2002.
- [4] M. Win and R. Scholtz, "Ultra-wide Bandwidth Time-Hopping Spread-Spectrum Impulse Radio for Wireless Multiple-Access Communications," IEEE Transactions on Communications, Vol. 48, No. 4, pp. 679-689, 2000.
- [5] Xiaomin Chen and S. Kiaei, "Monocycle Shapes for Ultra Wideband System," 2002 IEEE International Symposium on Circuits and Systems, Proceedings (Cat. No.02CH37353), Vol. 1, pp. I-597-I-600, 2002.
- [6] H. Yazdani, A. M. Rabiei and N. C. Beaulieu, "Multiaccess Interference Whitening for TH-BPSK IR-UWB Systems," 2012 26th Biennial Symposium on Communications(QBSC), Kingston, ON, pp. 111-114, 2012.
- [7] Richard A. Poisel, Modern Communications Jamming Principles and Techniques, Artech House Boston London.