논문 17-42-12-01 The Journal of Korean Institute of Communications and Information Sciences '17-12 Vol.42 No.12
https://doi.org/10.7840/kics.2017.42.12.2227

SDR을 이용한 디지털 신호에 대한 최적의 재밍 기법 성능 평가

박 찬 근◆, 최 신 욱*, 한 성 민*, 최 지 웅°

Performance Evaluation of the Optimal Jamming Method for Digital Signals Using SDR

Chankeun Park◆, Sinuk Choi*, Sungmin Han*, Ji-Woong Choi°

요 약

본 논문에서는 software defined radio (SDR) 기반의 universal software radio peripheral (USRP)를 이용하여 송수신부 및 재머를 구현하고 이를 이용한 실험을 통해 additive white Gaussian noise (AWGN) 재밍 기법, quadrature phase shift keying (QPSK) 재밍 기법 및 디지털 신호에 대한 최적의 재밍 기법의 성능 평가를 진행하였다. 실험 결과를 통해 디지털 신호에 대한 최적의 재밍 기법은 기존 재밍 기법 대비 실제 환경에서도 이득이 있음을 확인할 수 있었다.

Key Words : Jamming, digital communication, QPSK, Universal software radio peripheral, Optimal jamming, Software defined radio (SDR)

ABSTRACT

In this paper, we implemented a communication transceiver and jammer using universal software radio peripheral (USRP) based on software defined radio (SDR), and tested the receiver performance of three jamming methods including additive white Gaussian noise (AWGN) jamming, quadrature phase shift keying (QPSK) jamming, and the jamming scheme optimal to the digital signal. Through experiment results, we confirmed that the optimal jamming for digital signal is better than other conventional schemes in real environments.

Ⅰ. 서 론

통신 기술의 발달에 따라 현대전에서 전자전이 차지하는 비중이 증가하고 있다. 전자전의 한 요소인 재밍 기술은 의도적인 간섭 신호를 전송함으로써 적군의 통신을 교란시킬 수 있는 기술이다[1,2]. 효과적인 교란을 위해 가우시안 잡음 형태의 재밍 신호를 전송하는 AWGN 재밍, 임의의 QPSK 신호를 재밍 신호로 사용하는 QPSK 재밍 기법[3], 그 이외에 톤 재밍, 펄스 재밍, 주파수 추적 재밍 등 다양한 방법의 재밍 신호가 이용된다[2]. 일반적으로 채널 용량의 관점에서의 최적의 재밍 신호는 가우시안 분포를 따르지만, 디지털 신호의 bit error rate (BER) 관점에서의 최적 신호는 가우시안 분포를 따르지 않는 신호임이 증명된 바 있다[3]. 하지만 [3]의 결과는 평탄한 페이딩 채널 및 송수신기 와 재머 간의 완벽한 동기 등의 이상적

※ 이 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음.
◆ First Author : DGIST Department of Information and Communication Engineering, kkga111@dgist.ac.kr, 학생회원
° Corresponding Author : DGIST Department of Information and Communication Engineering, jwchoi@dgist.ac.kr, 종신회원
* DGIST Department of Information and Communication Engineering, lmy0829@dgist.ac.kr, krcapt13@dgist.ac.kr, 학생회원
논문번호 : KICS2017-10-303, Received October 12, 2017; Revised November 12, 2017; Accepted November 16, 2017

환경 하에서 가정한 상태에서 도출되었기 때문에 현실적 환경에서 [3]의 제안 방법의 신뢰성이 명확하지 않다. 따라서, [3]의 제안 방법을 실제 환경에 사용하기 앞서 실제 환경을 고려한 시뮬레이션 및 수식적 접근을 통한 성능 검증이 필수적이다. 하지만 실제 환경은 매우 많은 변수가 있기 때문에 컴퓨터 시뮬레이션 혹은 수식화를 통한 검증에 큰 어려움이 따른다. 따라서 본 논문에서는 유사한 실험 환경을 구현하여 [3]의 결과를 실제 환경에서 검증하였다.

이를 위해 두 대의 SDR을 이용하여 송수신단과 재머를 구현하고 이를 이용해 실제의 통신 환경에서 디지털 신호에 대한 최적의 재밍 기법에 대한 성능 평가를 진행하였다. 또한 비교를 위해 기존 AWGN 및 QPSK 재밍 기법에 대한 성능 평가 역시 진행하였다.

Ⅱ. 본 론

2.1 디지털 신호에 대한 최적의 재밍 기법

재밍 신호가 수신기에 미치는 영향은 재밍 신호의 평균 전력 및 순시 전력에 따라 다르다. 만일 평균 재밍 신호 전력이 평균 송신 신호 전력보다 매우 낮을 경우 지속적으로 재밍 신호를 가하더라도 기대할 수 있는 오류율은 매우 낮다. 따라서 송신 신호 전력이 매우 크고 평균 재밍 신호 전력을 유지해야 할 때 재머가 취할 수 있는 최적의 전략은 순시 전력을 높여 송신 신호의 비트 오류율을 높이는 것이다. 이와 같은 순시 전력 최적화는 [3]에서 유도된 바 있다. 유도된 디지털 신호에 대한 최적의 재밍 기법에 대한 재밍 신호의 확률 밀도 함수는 식 (1)로 표현된다[4].

$$f_{\bar{J}}(\bar{j}) = \lambda\delta(\bar{j}-\bar{j}^{(1)}) + (1-\lambda)\delta(\bar{j}-\bar{j}^{(2)}) \qquad (1)$$

여기서 λ의 범위는 $0 \leqq \lambda \leqq 1$이며, $\bar{j}^{(1)}$와 $\bar{j}^{(2)}$는 복소 재밍 신호를 뜻한다. 식 (1)은 재밍 신호의 확률 밀도를 나타내는 식이므로 λ의 확률로 $\bar{j}^{(1)}$를 전송하며 $(1-\lambda)$의 확률로 $\bar{j}^{(2)}$를 전송하는 것을 의미한다. 표 1은 재밍 신호 대 잡음비 (jamming to noise power ratio, JNR)가 10 dB일 때 QPSK 신호에 대한 비트에너지 대 잡음비 (Energy per bit to noise power spectral density ratio, E_b/N_0) 별 최적의 λ와 $\bar{j}^{(1)}$, $\bar{j}^{(2)}$를 나타낸다[3]. 이와 같은 확률 분포 하에서 송신 신호의 평균 전력이 높을 경우 재밍 신호는 대부분의 시간 동안 송신을 하지 않고 있다가, 낮을 확률로 재밍 신호 송신을 시도한다. 이와 같이 on-off 방식으로 재밍 신호를 전송할 경우 재밍 신호를 전송하는 순간의 순시 전력은 기존보다 상승하여 송신 신호에 비트 오류를 유발할 가능성이 높아진다. 따라서 평균 재밍 신호 전력이 송신 신호의 평균 전력보다 낮을 경우에는 재밍 신호가 오류를 유발하기 힘들기 때문에 약한 전력의 재밍 신호를 지속적으로 보내는 것보다 on-off 방식으로 재밍 신호의 순시전력을 높여 전송하는 것이 우수한 재밍 효과를 나타낼 수 있다. 예를 들어 JNR이 10 dB일 때 QPSK 신호에 대한 최적의 재밍 신호는 E_b/N_0이 0 dB에서 13 dB일 경우 임의의 QPSK 신호를 재밍 신호로써 전송하고, 15 dB이상의 E_b/N_0에서는 on-off 방식으로 재밍 신호를 전송하는 것이 최적이다.

표 1. JNR이 10dB 일 때 QPSK 신호에 대한 최적의 재밍 기법
Table 1. Optimal jamming method for QPSK signals when JNR is 10dB

E_b/N_0(dB)	λ	$\bar{j}^{(1)}$	$\bar{j}^{(2)}$
$0 \sim 13$	1	$\pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}$	$\pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}$
15	0.359	$\pm\frac{1}{\sqrt{2\lambda}} \pm j\frac{1}{\sqrt{2\lambda}}$	0
18	0.184		
21	0.099		
24	0.049		
27	0.027		
30	0.012		

위와 같이 on-off 방식으로 재밍 신호를 전송하더라도 일정 시간에 대한 평균 재밍 전력은 전 구간의 E_b/N_0 값에서 동일하다. 왜냐하면, E_b/N_0가 0 dB에서 13 dB일 때의 복소 재밍 신호 $\bar{j}^{(1)}$과 $\bar{j}^{(2)}$의 전력보다 on-off 방식에서 신호를 보내는 $\bar{j}^{(1)}$ 신호가 더 전력이 세고, $\bar{j}^{(2)}$가 선택되었을 때는 신호를 전송하지 않기 때문에 전력이 0이 되어 일정 시간에 대한 평균 전력은 전 구간에서 동일하다. 따라서 JNR은 E_b/N_0값에 관계없이 모든 구간에서 일정 시간에 대한 평균 재밍 신호의 전력이 동일하기 때문에 본 실험에서는 JNR을 10 dB로 일정하게 유지하였다.

2.2 송수신단과 재머의 구현

본 연구에서는 송수신단과 재머를 구현하기 위해서 두 대의 National Instruments (NI) USRP-2901 모델과 VERT2450 안테나 세 개를 사용하였다. 본 실험에

서는 USRP의 중심 주파수를 2.4 GHz로 설정하였고, 신호 전송 시송신 전력은 -50.66 dBm, 수신기에서는 30 dB의 이득을 가지도록 설정하였다. 안테나는 2.4 ~ 2.48 GHz, 4.9 ~ 5.9 GHz의 이중 대역을 지원하며, 3 dBi의 안테나 이득을 가진다.

송신단의 구성은 그림 1과 같이 송신단의 포트 1을 통해 QPSK 변조 방법을 사용한 전송 신호를 송신하였고, 포트 2에서는 포트 1에서 보내는 신호에 간섭을 가하는 재머 및 의사 잡음 생성기 신호를 송신하기 위해 사용되었다. 실제 잡음 신호보다 의사 잡음 신호의 전력이 매우 크므로 실제 수신기의 잡음은 의사 잡음으로 근사화할 수 있다.

수신단은 송신 신호, 재밍 신호 및 의사 잡음 신호 모두를 하나의 포트를 사용하여 수신하여, 자동 이득 제어, 정합 필터, 위상 동기 루프, 타이밍 동기 루프, QPSK 디코더, 그리고 프레임 동기의 블록단으로 구성된다[4,5].그리고 위상 동기 루프에서 위상 에러를 검출하기 위해서 비 데이터 도움 최대 우도 검출기를 사용하였으며, 타이밍 동기 루프에서 타이밍 오류를 검출하기 위해서 비 데이터 도움 영점 교차 검출기를 사용하였다[5]. 본 논문에서는, 재머가 BER에 미치는 영향만을 확인하기 위하여 프레임 동기에 오류가 발생하였을 경우 최종 BER 계산 시 고려하지 않았다. 두 기기 간의 동기는 맞지 않으므로 송신단의 포트 1에서는 프레임 동기를 맞추기 위하여 데이터 신호 앞에 자기 상관 특성이 우수한 코드 길이 13의 바커 코드를 헤더로 붙여서 전송하였다[4]. 각 재밍 기법 별로 송신 신호에 직접적인 영향의 정도를 확인하기 위하여 어떠한 항재밍 기법도 수신단에서 사용하지 않는 상황을 가정하였다[3]. 또한 최대한 동일한 채널상태를 만들기 위해서 유동 인구가 적은 실험실에서 실험을 진행하였다.

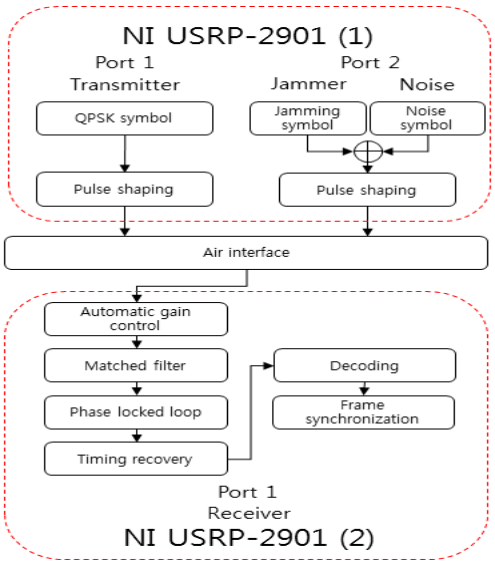

그림 1. 구현된 송수신단과 재머의 블록도
Fig. 1. Block diagrams of the implemented transmitter, receiver, and jammer

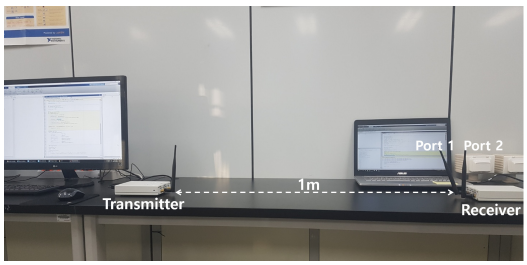

그림 2. 재밍 신호 분석용 실험 환경
Fig. 2. Experiment environment for jamming signal analysis

Ⅲ. 실 험

그림 3은 QPSK 송신 신호에 대한 최적의 재밍 기법, AWGN 재밍 기법, 그리고 QPSK 재밍 기법에 대한 실험 결과이다. 성능에 대한 척도로는 BER이 사용되었으며 JNR은 10 dB로 고정하였다. 송신 신호의 E_b/N_0 값이 0 dB에서 12 dB인 구간에서는 QPSK 재밍 기법과 유사하게 재밍 신호를 전송하기 때문에 최적 재밍 기법의 BER과 기존 AWGN 재밍, QPSK 재밍 기법들의 BER이 비슷한 값을 가지는 것을 확인할

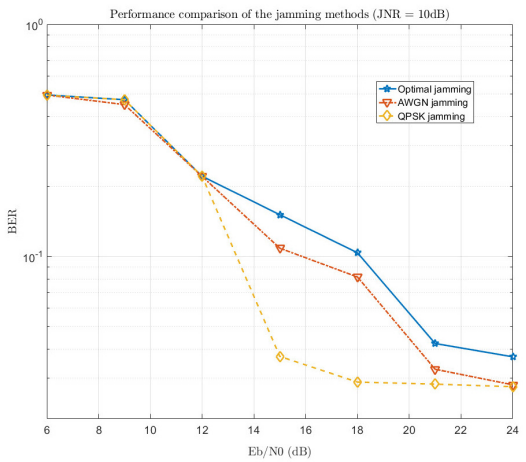

그림 3. QPSK 신호 송신 시 재밍 실험 결과
Fig. 3. BER performance in presence of the jamming signal under QPSK signal transmission

수 있다. 최적의 재밍 기법에서는 E_b/N_0 값이 13 dB 일 때부터 재밍 신호 전송 방법이 on-off 방법으로 바뀌는데, 그림 3에서는 E_b/N_0 값이 12 dB일 때부터 재밍 기법 별 BER 성능 열화 차이가 발생하는 것처럼 보인다. 이는 실험을 진행할 때 E_b/N_0 측정 간격을 3 dB로 설정하였기 때문에 12 dB부터 최적의 재밍 기법의 BER 성능 차이가 발생하는 것처럼 보인다. 하지만 실제로는 13 dB부터 재밍 기법 간 BER 차이가 발생할 것이다. 신호의 E_b/N_0 값이 약 20 dB이상의 값을 가질 경우 JNR이 10 dB로 제한된 환경에서 on-off 방식으로 재밍 신호를 전송하여도 송신 신호의 비트 에너지가 강하여 재밍 신호가 오류를 유발하기 힘들기 때문에 다른 재밍 기법들과 같이 수신단의 BER 값이 크게 감소한다.

14 dB 이상의 E_b/N_0에서 QPSK 재밍 기법은 AWGN 재밍 기법보다 재밍 성능이 크게 좋지 못한 것을 볼 수 있다. QPSK 재밍 기법은 $\lambda=1$의 최적 기법과 같으므로, λ가 잘못 설정되었을 경우 최적 재밍 기법의 성능 열화가 극심함을 의미한다. 그러므로 최적의 재밍 기법을 사용하고자 한다면 현재의 E_b/N_0가 on-off 방식으로 넘어가는 임계값을 넘어갔는지 아닌지를 정확히 판단할 수 있어야 한다.

Ⅳ. 결 론

본 논문에서는 실제적인 환경에서 디지털 신호에 대한 최적의 재밍 기법의 성능을 평가하고자 NI USRP-2901를 이용하여 실험을 진행하였다. 기존 연구의 시뮬레이션 결과에서 보여주는 것과 마찬가지로 실제의 제한된 환경에서 실험을 하였을 때, 유도된 최적의 재밍 기법이 일반적인 다른 재밍 기법들(AWGN 및 QPSK 재밍) 보다 더 효과적으로 통신을 교란시키는 것을 볼 수 있었다. 따라서 최적 재밍 기법을 사용하면 다른 재밍 기법들보다 실제 환경에서도 더 나은 성능을 기대할 수 있다. 본 논문에서는 재밍 신호에 따른 데이터의 복조 성능 저하를 비교하기 위해 동기 오류 프레임이 발생하지 않은 상황을 고려하였으며, 동기 성능 차이와 영향 등에 대해서도 추후 연구를 진행할 예정이다.

References

[1] K. Y. Kim, "Analysis of anti-jamming techniques for satellite navigation systems," *J. KICS*, vol. 38, no. 12, pp. 1216-1227, Dec. 2013.

[2] J. M. Rhee, *Military communication system*, Hongrung Publishing, pp. 319-348, 2014.

[3] S. Amuru and R. M. Buehrer, "Optimal jamming strategies in digital communications – Impact of modulation," in *Proc. Globecom*, pp. 1619-1624, Austin, TX, USA, Dec. 2014.

[4] D. A. Cuji, P. A. Chasi, F. Guerrero, and F. Rivera, "Frame synchronization through barker codes using SDRs in a real wireless link," in *Proc. CONIELECOMP*, pp. 68-72, Cholula, Mexico, Feb. 2016.

[5] M. Rice, *Digital communications - A discrete-time approach*, Pearson, pp. 359-518, 2009.

박 찬 근 (Chankeun Park)
2015년 8월 : 가톨릭대학교 정보통신전자공학부 졸업
2017년 8월 : DGIST 정보통신융합전공 석사
2017년 9월~현재 : 국방과학연구소 연구원

최 신 욱 (Sinuk Choi)
2017년 2월 : 경북대학교 전자공학부 졸업
2012 3월~현재 : DGIST 정보통신융합전공 석사과정

한 성 민 (Sungmin Han)
2012년 2월 : 한국기술교육대학교 전자공학과 졸업
2012년 3월~현재 : DGIST 정보통신융합전공 석박사 통합과정

최 지 웅 (Ji-Woong Choi)
1998년 2월 : 서울대학교 전기공학부 졸업
2000년 2월 : 서울대학교 전기공학부 석사
2004년 8월 : 서울대학교 전기컴퓨터공학부 박사
2004년 9월~2005년 10월 : 서울대학교 반도체 공동연구소 박사후연구원
2005년 10월~2007년 7월 : Stanford Univ. 박사후연구원
2007년 8월~2010년 10월 : Marvell Semiconductor 책임연구원
2010년 10월~현재 : DGIST 정보통신융합전공 교수