논문 17-42-11-01 The Journal of Korean Institute of Communications and Information Sciences '17-11 Vol.42 No.11
https://doi.org/10.7840/kics.2017.42.11.2069

주파수 도약 확산 스펙트럼 시스템에서 CFAR 검출기를 이용한 항재밍 영향 성능 분석

이 호 준◆, 김 성 호*, 정 재 학°

Performance Analysis of Anti-Jamming by CFAR Detector in Frequency-Hopping Spread Spectrum Systems

Hojun Lee◆, Sungho Kim*, Jaehak Chung°

요 약

군사적 목적의 무선 통신 시스템은 적에 의한 재밍 공격 등에 의해 간섭을 받아 수신 신호 복호시에 신뢰성을 보장할 수 없기 때문에 복수의 동일한 데이터를 가지는 다중 슬롯을 보내고 이를 수신단에서 결합하여 재밍의 영향을 줄인다. 본 논문에서는 Freqeuncy Hopping Spread Spectrum(FHSS)를 이용하여 재밍 신호를 회피하는 알고리즘의 경우에 간섭이 발생한 슬롯을 검출하기 위해 Cell Average Constant False Alarm Rate (CA-CFAR) 검출 알고리즘을 이용하여 재밍 신호를 검출하고 나머지 동일한 데이터를 가지는 슬롯 들에 대한 부분 결합 기법을 이용해 높은 신뢰성을 보장하는 알고리즘을 제안한다. 그리고 전산 모의실험을 통해 제안된 알고리즘이 FHSS환경에서 false alarm rate 을 변화할 때 재밍 검출 성능을 분석하였고, 비트 에너지(E_b)와 재밍 신호의 전력 밀도(J_0)의 비율인 E_b/J_0이 변화할 때 검출 성능 변화에 따라 Bit Error Rate(BER)이 연관되어 변화하는 것을 보였다. 이러한 실험 분석을 통해 제안한 알고리즘이 기존의 모든 슬롯을 결합하는 방법에 비해 BER성능이 향상되었음을 보였다.

Key Words : Jamming, Jammer, FHSS, CFAR, False Alarm Rate, DQPSK

ABSTRACT

In military environment, wireless communication systems does not guarantee reliability due to the effect of interference by a jamming attack. To reduce the influence of the jamming attack, transmitter sends identical signal in some slots by using Frequency Hopping Spread Spectrum(FHSS) and receiver combines that received slots. This paper proposes the Cell Average Constant False Alarm Rate(CA-CFAR) detection algorithm to remove the received slot attacked by the jammer, and utilizes the selection-combining technique to increase array gain. Computer simulation demonstrates jamming detection performance as a function of the false alarm rate and jammer bandwidth for the FHSS, and shows Bit Error Rate(BER) performance as a function of the ratio of bit energy(E_b) to the power spectral density(J_0). Computer simulation proves the proposed method exhibits better BER performance than the conventional combining method.

※ 본 논문은 한화시스템(과제번호 : S-16-004)의 지원을 받아서 작성되었습니다.
◆ First Author : Inha University Department of Electronic Engineering, timmit@naver.com, 학생회원
° Corresponding Author : Inha University Department of Electronic Engineering, jchung@inha.ac.kr, 종신회원
* 한화시스템연구원, zeulja.kim@hanwha.com
논문번호 : KICS2017-09-233, Received September 4, 2017; Revised October 26, 2017; Accepted October 26, 2017

Ⅰ. 서 론

무선 통신은 동일 주파수 대역을 사용하는 다른 신호들로 인해 전파 방해를 받을 경우 전송 성능 이 저하된다. 특히 그림 1과 같이 군사적 환경에서의 무선 통신 시스템은 적에 의해 송신 신호의 주파수와 같은 대역에 강한 신호를 주입하는 재밍 공격에 취약하다[1,2]. 군사적 목적의 무선 통신 시스템은 높은 신뢰성을 요구하기 때문에 재밍 공격으로부터 발생하는 간섭 효과를 제거해야 한다.

재밍 신호의 전력은 대역폭에 반비례하므로 같은 전력의 재밍 신호에서 광대역 재밍 신호는 상대적으로 전파 방해 효과가 적기 때문에 일반적으로 전파 방해에 사용하는 재밍 신호는 협대역이다[2,3]. 협대역 재밍 신호로 인한 간섭 영향을 줄이기 위한 기법으로는 할당된 주파수 대역 내에서 시간에 따라 무작위로 반송 주파수를 변화시켜 전송하는 기법인 Frequency Hopping Spread Spectrum (FHSS)과 전송하는 신호에 Pseudo-random Noise(PN) 시퀀스를 곱하여 전송하고 수신된 신호를 해당 PN 시퀀스와 correlation을 통해 신호를 복원하는 Direct Sequence Spread Spectrum(DSSS) 등과 같은 기법 및 이를 응용한 연구가 진행되어왔다[4-10].

FHSS 기법은 시간에 따라 무작위로 반송 주파수를 변화시켜 전송하는 기법이기 때문에 확률적으로 전송하는 신호의 일부분은 재밍 신호의 주파수대역과 겹쳐지게 되어 간섭이 발생하게 된다. 협대역 재밍 신호는 비교적 강한 신호이므로 간섭이 발생한 주파수 대역의 신호를 복원하기 어렵다. 따라서 높은 신뢰성을 보장하기 위해 여러 슬롯에 같은 데이터를 전송하는 repetition 기법을 이용하여 전송하고 수신단에서 이를 결합으로써 diversity 이득을 얻는다[3]. 그러나 반복된 신호를 복원할 때, 강한 재밍 신호로 인하여 간섭이 발생한 주파수 대역의 신호를 함께 결합하게 되면 원하는 신호로 복원하기 어렵다. 따라서 간섭이 발생한 주파수 대역의 신호를 제외하고 결합하는 기법을 이용한다[11]. 그러나 수신 신호 슬롯 중에서 재밍 신호가 더해졌는지 판단하는 것은 어렵다.

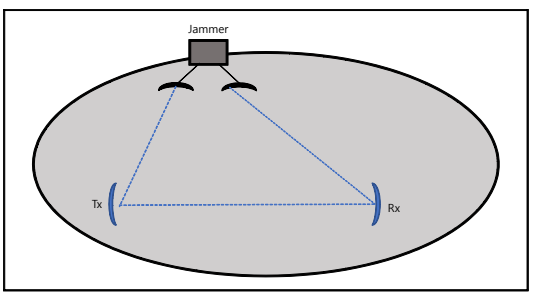


그림 1. 송수신기와 재머의 기하학적인 형태
Fig. 1. Geometric representation of the transmitter, Receiver and jammer

본 논문에서는 협대역 잡음 재밍 환경 하에서 Constant False Alarm Rate(CFAR) 검출 기법을 이용하여 슬롯내의 재밍 신호를 검출하는 방법을 사용하며 false alarm rate (P_{fa})의 변화에 따른 재밍 신호 검출 성능과 이를 바탕으로 반복되는 슬롯을 결합하였을 때 수신 성능 변화를 분석하였다. CFAR 검출 기법은 P_{fa}를 일정하게 유지하기 위한 적응형 임계 값이 있는 검출 기법으로[12] 가장 잘 알려진 것이 CA-CFAR이다. 이 기법은 백색 가우시안 잡음 하에서 최적의 성능을 보이지만 비균일 잡음 하에서는 성능이 저하되기 때문에 SO-CFAR 기법이 연구되었다[13-15]. 본 논문의 실험에서는 이 두 가지 검출기에 대해서 P_{fa}을 변경하면서 재밍 신호의 검출 성능을 분석하고 이에 바탕으로 수신단에서 슬롯의 결합을 한 뒤 얻어지는 비트오류율(Bit Error Rate: BER)을 보였다.

본 논문의 구성은 2절에서 시스템 모델을 설명한 후 3장에서 제안된 알고리즘을 설명하고 4장에서 전산 모의실험을 통해 제안한 알고리즘의 성능을 보이고 5장에서 결론을 맺는다.

Ⅱ. 시스템 모델

본 논문에서 사용하는 재밍 신호를 회피하기 위한 기법 중 하나인 FHSS는 사전에 송수신단에서 정한 hopping 패턴을 이용하여 반송 주파수를 시간에 따라 바꾸어 전송하는 기법으로 일반적으로 hopping 패턴은 PN 시퀀스로 설정하며 데이터를 송수신하기전에 hopping 패턴을 공유한다.

그림 2에서 $M(k)$는 k번째 비트의 송신 데이터 그리고 $M'(k)$는 수신된 신호를 복원한 데이터이다. 송신단에서 변조된 심볼의 시간 간격을 T_s 그리고 반송 주파수가 변화되는 간격인 슬롯 간격을 T_c라 하며 $T_c \geq T_s$ 인 경우는 slow FHSS라 하고 $T_c < T_s$인 경우는 fast FHSS라 한다. 본 논문에서는 slow FHSS를 사용한다. 그림 2에서와 같이 송신단에서 변조된 신호에 대하여 hopping 패턴에 의해 결정된 반송 주파수로 변환하여 주파수 도약을 한 후 신호를 전송한다. 주파수 도약과 합성하는 과정인 $h_{fh}(t)$는 다음 식

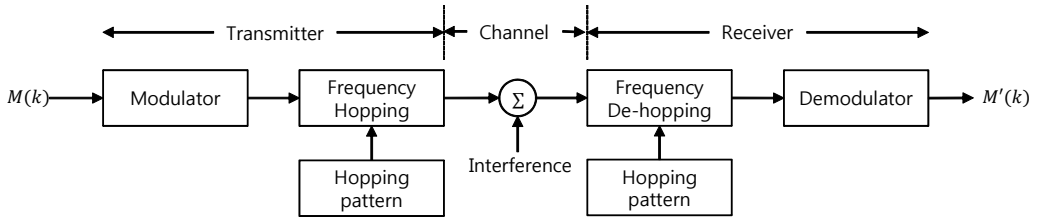


그림 2. FHSS 블록도
Fig. 2. Block diagram of FHSS

으로 표현할 수 있다[16].

$$h_{fh}(t)=\sum_{n} p(t-nT_c)\cos(2\pi f_n t+\phi_n) \quad (1)$$

여기서 f_n와 ϕ_n은 n번째 슬롯의 반송 주파수와 위상이며 $p(t)$는 $p(t)=u(t)-u(t-T_c)$이며 $u(t)$는 단위 계단 함수이다. 그리고 송신 신호 $s_{fh}(t)$는 다음 식으로 표현된다.

$$s_{fh}(t)=s(t)\,h_{fh}(t) \quad (2)$$

여기서 $s(t)$는 변조된 신호이다. 수신단에서는 송신단과 반대 과정으로 주파수 도약된 신호를 복조한 후 원하는 데이터인 $M'(k)$를 얻는다. 전송하는 신호는 수신단에서 채널 추정 없이 검출을 용이하게 하기 위해서 differential m-PSK를 사용한다.

그림 3은 재밍 신호가 존재할 때 $T_c=T_s$에 해당하는 slow FHSS를 시간-주파수 영역으로 나타낸 것이다. 전체 주파수 대역을 B, 주파수 도약된 개별 신호의 주파수 대역을 B_h 그리고 재밍 신호의 주파수 대역을 B_j라 하며 할당된 반송 주파수를 $f_1,\cdots,f_8$로 표기하였다.

FHSS 기법을 사용하더라도 일부 주파수 대역은 확률적으로 재밍 공격으로부터 회피하지 못하여 간섭이 발생하게 된다. 재밍 신호의 전력량은 대역폭과 시간에 곱에 비례하므로 고정된 전력을 갖는 재밍 신호의 Power Spectral Density(PSD) J_0은 대역폭에 반비례하게 된다. 본 논문에서 사용하는 정보 비트 당 신호 에너지인 E_b와 J_0의 비율인 E_b/J_0은 다음 식으로 표현된다.

$$\frac{E_b}{J_0}=\frac{S/f_b}{J/B_j}=\left(\frac{S}{J}\right)\left(\frac{B_j}{f_b}\right)=\left(\frac{S}{J}\right)\left(\frac{\rho B}{f_b}\right) \quad (3)$$

여기서 S는 신호의 전력, J는 재밍 신호의 전력, f_b는 채널 전송률 그리고 전체 주파수 도약 대역에서 재밍 신호가 차지하는 상대적인 대역의 비율인 ρ는 B_j/B로 정의 된다.

송신 신호의 전력과 재밍 신호의 전력이 고정되어 있을 때 ρ에 따라 E_b/J_0이 변화한다. 잡음의 PSD를 N_0이라고 하면 재밍으로부터 간섭이 발생한 대역의 잡음전력밀도는 $E_b/(N_0+J_0)$이 된다. 이 $E_b/(N_0+J_0)$은 ρ에 따라 결정되며 ρ가 작은 값을 가질 때 재밍 신호로 인한 영향이 커지게 되고 $E_b/(N_0+J_0)$이 작아지므로 BER 성능이 저하된다.

FHSS 기법은 각각의 hop에 의한 슬롯에 해당하는 반송 주파수가 다르기 때문에 각각의 슬롯 대한 채널이 다르다. 따라서 수신단에서 각각의 슬롯에 대하여 채널 추정 및 등화기를 개별적으로 설계하여야 하기 때문에 복잡도가 증가한다. 또한 FHSS 기법의 특성상 전체 주파수 대역을 효율적으로 사용할 수 없어 전송률이 떨어지게 되는데 각각의 슬롯의 채널 추정을 개별적으로 해야 하므로 채널추정을 위한 파일롯으로 인해 전송률이 더욱 저하된다. 이러한 문제를 보완하기 위해 Differential Quadrature Phase Shift Keying (DQPSK) 변조방식을 이용한다. DQPSK는 이전 심

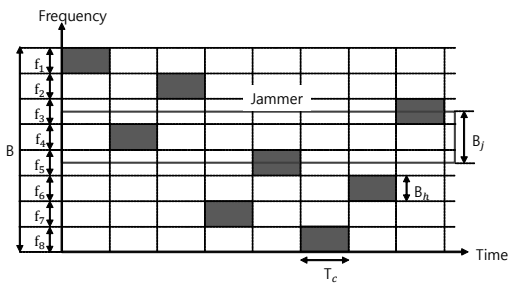


그림 3. 재밍 신호 하에서 slow FHSS 기법의 시간-주파수 영역
Fig. 3. Time-frequency domain of the slow FHSS with the jamming signal

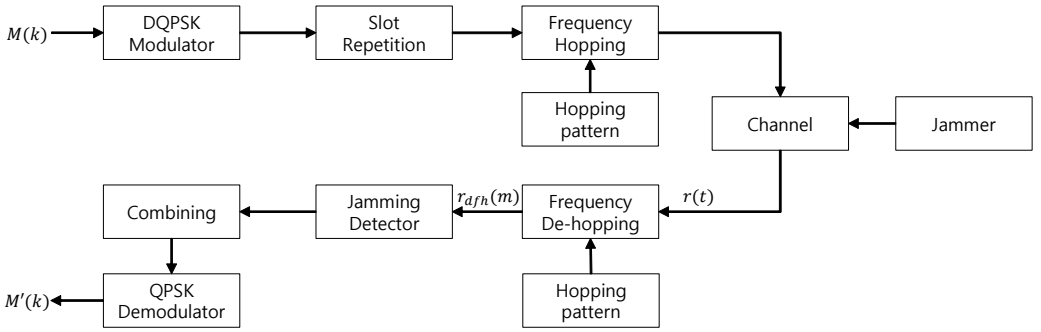


그림 4. 제안한 방법의 블록도
Fig. 4. Block diagram of the proposed method

볼과 현재 심볼 간의 위상 차이를 이용하여 복조하기 때문에 채널 추정 및 등화기를 설계할 필요가 없으므로 복잡도 및 파일롯으로 인한 전송률 손실을 보상할 수 있다.

이러한 FHSS의 경우 재밍의 영향을 줄이기 위해 여러 슬롯에 동일한 데이터를 전송하는 repetition 기법과 channel coding을 이용하는 기법이 있다. Repetition을 이용하여 전송하는 경우 수신단에서 간섭이 발생한 주파수 대역의 슬롯을 제외하고 결합함으로써 diversity 이득을 얻어 신호를 복원한다. Channel coding을 이용하여 전송하는 경우 수신단에서 간섭이 발생한 슬롯을 제거한 후 decoding 함으로써 원래의 신호로 복원한다. 후자의 경우는 전자에 비해 높은 전송률을 갖고 diversity와 coding 이득을 얻을 수 있기 때문에 성능 측면에서는 유리하다. 그러나 channel coding으로 인해 발생하는 복잡도가 증가하는 단점이 있다. 본 논문에서는 높은 전송률을 요구하지 않으면서 매우 간단한 복호기를 이용하는 군사적 시스템에 적용하기 위해 repetition 기법을 이용한다.

단순 결합을 통하여 수신 신호를 복원할 경우에 재밍 신호가 강한 경우에는 복호 성능이 더 나빠지게 된다. 이 경우 재밍이 더해진 슬롯을 제외하고 결합하면 수신 단에서 복호 성능을 올릴 수 있는데 이때 슬롯에 재밍이 존재하는지를 검출하는 것이 관건이다. 일반적으로 다른 슬롯의 평균 전력보다 일정 전력이상 큰 경우를 가정하는 고정 임계 값을 이용한 검출 방식으로 재밍 슬롯을 검출하여 수신단에서 슬롯 결합에서 제외시킨다. 그러나 이 방법은 변화하는 슬롯의 전력 변화 값에 대응하기 어려운 문제가 있어서 본 논문에서는 임계 값이 슬롯의 전력 변화에 적응적으로 변화하면서 항상 일정한 P_{fa}을 가지는 CFAR 검출기를 이용하여 재밍이 더해진 슬롯인지 검출한다. 다름 절에는 CFAR를 이용하여 수신된 슬롯에 재밍 신호의 존재 유무를 검출하는 방법에 대해서 설명한다.

Ⅲ. CFAR을 이용한 재밍 검출 방법

그림 4는 본 논문에서 사용하는 CFAR 검출기를 이용하여 재밍이 더해진 슬롯을 검출하고 이것을 슬롯 결합 시 배제시키는 방법을 나타낸 블록도이다. 송신하고자 하는 데이터를 DQPSK 변조한 후 FHSS 기법을 이용하여 여러 슬롯에 같은 데이터를 hopping하여 전송한다. 수신된 신호는 전송과정에서 발생하는 재밍에 의해 신호가 왜곡될 수도 있다. 수신단에서는 Frequency de-hopping을 통해 passband 신호를 baseband 신호로 변환한 후 재밍 신호로부터 간섭이 발생한 신호를 검출하여 제거한 후 같은 데이터를 가지고 있는 여러 슬롯 데이터를 결합하여 신호를 복원한다.

본 논문에서 사용하는 재밍 신호 검출 기법은 CFAR 검출 기법으로 주로 레이더 시스템에서 사용되는 방법과 유사하다. CFAR 검출 기법은 P_{fa}를 일정하게 유지하며 임계 값이 주변 신호들의 변화에 적응적으로 변화하며 검출하는 기법인데 CA-CFAR가 대표적이다. 본 논문은 CA-CFAR 검출 기법을 재밍 검출 알고리즘으로 이용하는 기법을 제안한다.

그림 5에 그림 4의 jamming detector에서 사용된 CA-CFAR 검출 기법의 블록도를 나타내었다. 주파수 도약에 사용된 슬롯은 수신단에서 기저대역으로 변환시키기 때문에 기저대역에서는 슬롯의 구분이 없이 연속적인 데이터를 얻을 수 있고 이때 m번째 심볼을 $r_{dfh}(m)$라 한다. 이 데이터들의 각각 심볼들은 재밍 신호가 존재하는지 검사하기 위해 이 연속적인 데이터를 순차적으로 각각 training cell과 guard cell 그리

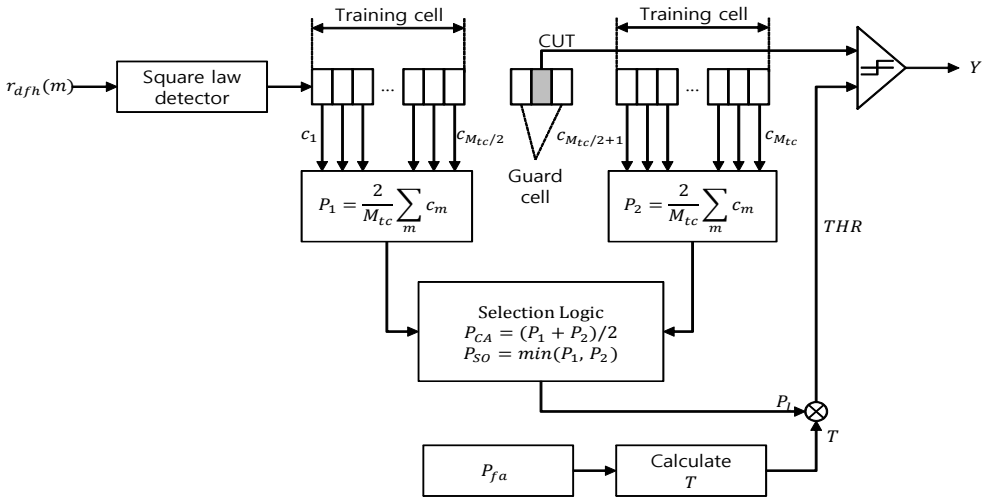


그림 5. CA-CFAR 블록도
Fig. 5. Block diagram of the CA-CFAR

고 CUT(Cell Under Test)에 한 심볼 간격으로 이동시켜가며 CFAR의 입력으로 사용한다. 여기서 cell은 CFAR 입력으로 들어간 신호 구간의 심볼들을 의미한다. Guard cell과 training cell은 임계 값과 비교하는 값인 CUT의 양방향에 구성되어 있으며 guard cell은 CUT의 신호가 training cell에 누출되는 것을 방지하는 역할을 하며 training cell은 주변신호전력을 추정한다. 추정된 주변신호전력을 통해 임계 값을 계산하고 CUT와 비교하여 재밍 신호를 검출한다. 만일 재밍 신호가 검출되었다면 그 검출된 위치를 포함하는 슬롯을 재밍 신호가 존재하는 슬롯으로 가정하여 신호 결합 시 제외시킨다.

CA-CFAR 검출 기법은 주변신호가 Wide Sense Stationary(WSS) zero mean white complex gaussian 신호를 가정한 것으로 square law detector를 통과시키면 출력 값의 확률밀도함수 (Probability Density Function: PDF)는 exponential 분포를 따르게 되며 평균은 σ_N^2이다. 따라서 주변신호전력인 분산 값을 추정할 수 있음을 알 수 있으며 각각의 training cell에서 추정한 주변신호전력은 다음 식으로 표현된다.

$$P_1 = \frac{2}{M_{tc}} \sum_{m=1}^{M_{tc}/2} c_m \tag{4-1}$$

$$P_2 = \frac{2}{M_{tc}} \sum_{m=\frac{M_{tc}}{2}+1}^{M_{tc}} c_m \tag{4-2}$$

여기서 P_1과 P_2는 각각 CUT로부터 왼쪽과 오른쪽에 있는 training cell에서 추정한 잡음 전력이고, M_{tc}는 training cell의 수이다.

CA-CFAR의 종류에 따라 추정된 주변신호전력 P_l의 selection logic이 달라진다. CA-CFAR의 추정된 주변신호전력은 $P_l = (P_1 + P_2)/2$이고CA-CFAR에서 주변신호전력을 잘못 측정할 때 발생하는 문제를 개선하기 위해 좌우 training cell에서 작은 값을 주변신호전력으로 추정하는 SO-CFAR의 추정된 주변신호전력은$P_l = \min(P_1, P_2)$이다.

P_{fa}는 다음 식을 통해 계산할 수 있다.

$$\begin{aligned} P_{fa} &= \int_{V_T}^{\infty} f(x)dx \\ &= 1 - \int_{-\infty}^{V_T} f(x)dx \\ &= 1 - F(V_T) \end{aligned} \tag{5}$$

여기서 $f(x)$는 square law detector를 통과한 신호의 PDF이고 V_T는 이론상의 임계 값이며 $F(c)$는 누적분포함수 (Cumulative Distribution Function: CDF)이다. CDF인 $F(c)$는 다음 식으로 표현된다.

$$\begin{aligned} F(c) &= 1 - e^{-\frac{c}{\sigma_N^2}} \\ &= 1 - \frac{1}{\left(1 + \frac{c}{M_{tc}\sigma_N^2}\right)^{M_{tc}}} \end{aligned} \tag{6}$$

여기서 식 (6)는 샘플 수 M_{tc}일 때의 CDF를 나타낸 식이다. 식 (5)에 식 (6)를 대입하면 임계 값 V_T는 다음과 같이 나타난다.

$$V_T = \sigma_N^2 M_{tc}(P_{fa}^{-1/M_{tc}} - 1) \quad (7)$$

위 식에서 σ_N^2를 제외한 부분인 $M_{tc}(P_{fa}^{-1/M_{tc}} - 1)$를scale factor, T 라 한다. CA-CFAR에서 샘플 수는 training cell의 심볼 개수이다. 추정한 주변신호전력 P_l과 T를 곱함으로써 임계 값 THR을 얻을 수 있다.

$$THR = P_l T \quad (8)$$

계산된 임계 값과 CUT를 비교하여 $CUT \geq THR$이면 Y=0, $CUT < THR$이면 Y=1으로 재밍 신호로 인해 간섭이 발생한 신호는 CA-CFAR 검출 결과 값으로 0을 갖고 그 외의 신호는 1을 갖는다. 그러나 간섭이 발생한 신호를 모두 찾는 것은 어렵다. 따라서 각 슬롯 내에 검출된 신호가 존재하면 해당 슬롯에 재밍 신호가 존재하는 것으로 추정한다.

그림 4의 CFAR 검출기를 사용한 Jamming Detector 블럭을 통해 재밍 신호가 존재하는 슬롯을 검출한 뒤 Combining 블록에서는 수신 신호의 수신 신호 전력 이득을 높이기 위해 재밍이 존재하지 않는 슬롯을 제외시킨 후 나머지 슬롯에 대해 신호 검출을 위한 결합을 한다. Differential m-PSK는 앞 뒤 심볼 간의 위상차에 정보를 담고 있으므로 결합 수행 이전에 각 슬롯 내에 존재하는 신호의 위상차를 계산하여야 하며 n번째 슬롯에 m번째 심볼의 위상차인 $S^n(m)$는 다음 식으로 구할 수 있다.

$$S^n(m) = r_{dfh}^n(m)\left\{r_{dfh}^n(m+1)\right\}^* \quad (9)$$

여기서 $r_{dfh}^n(m)$는 frequency de-hopping을 통해 얻어진 연속적인 심볼들 중 n번째 슬롯의 m번째 심볼이다. 식 (9)의 결과로 이전 심볼과 현재 심볼간의 위상 차이와 심볼 에너지를 얻을 수 있다. 슬롯들을 결합한 후의 m번째 결합된 심볼 $S_{comb}(m)$는 다음 식으로 얻을 수 있다.

$$S_{comb}(m) = \sum_{n \in N_c} S^n(m) \quad (10)$$

여기서 N_c는 CFAR 검출기로부터 재밍 신호가 검출되지 않은 슬롯들의 집합을 의미한다. 식 (10)로 부터 얻어진 결합된 심볼은 위상 차이와 심볼 에너지를 통해 결합한 것이므로 maximum-ratio combining이 되며 QPSK와 동일하므로 QPSK 복조를 이용하여 원래 신호로 복원한다.

이와 같이 재밍의 효과를 줄이기 위해 DQPSK 변조방식을 사용하는 FHSS로 재밍 신호를 회피하고 FH을 하더라도 재밍의 영향을 받는 슬롯이 발생하기 때문에 여러 개의 반복된 슬롯을 전송하고 수신신호 복원 시 재밍의 영향을 받은 슬롯을 CFAR 검출기로 검출하여 수신신호 결합 시에 재밍 슬롯을 제외함으로써 재밍으로 인해 저하되는 성능을 개선하는 알고리즘을 제안하였다.

Ⅳ. 전산 모의실험

본 장에서는 표 1에 나타낸 실험환경에 대하여 제안된 재밍 검출 알고리즘을 이용하여 재밍을 검출한 후 슬롯을 결합하는 방법의 성능을 보이기 위해 기존의 모든 슬롯을 결합하는 방식과의 BER 비교를 한다. 그리고 제안한 방법의 성능에 영향을 주는 P_{fa}와 재밍 신호의 상대적 대역 비율인 ρ를 변화시키면서 제안된 알고리즘의 재밍 신호 검출 성능 및 수신 BER 성능을 분석하는 전산 모의실험을 수행한다.

그림 6은 그림 4에서 FHSS 송신 신호에 해당하는 spectrogram의 예이며, 그림 7은 채널을 통과하면서 E_b/J_0이 10dB, $\rho = 0.05$인 협대역 잡음 재밍 신호로

표 1. 실험 환경
Table. 1. Simulation conditions

Bandwidth	1MHz
Modulation scheme	$\pi/4$ DQPSK
Repetition	4
Each hop bandwitdh	250kHz
Symbol duration	50μs
Eb/No	16dB
ρ	0.005, 0.05
Channel model	Rician channel (K=10dB, $f_{d\max}$=3kHz)
Number of Training Cells	2*Number of symbols in a slot
Number of Guard Cells	Number of symbols in a slot
False Alarm Rate (P_{fa})	$10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}$

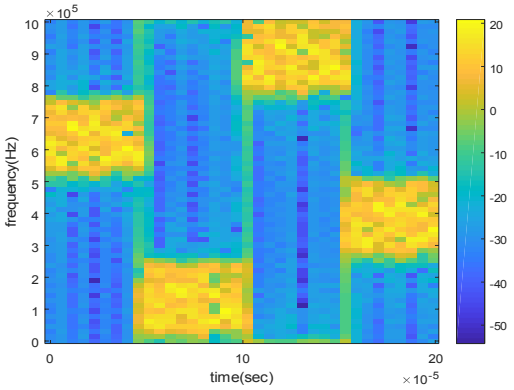


그림 6. FHSS 송신단 신호 spectrogram
Fig. 6. Spectrogram of the transmitted signal for FHSS

인해 간섭이 발생한 신호의 spectrogram이다. 두 번째 슬롯에 해당하는 신호가 재밍 신호를 회피하지 못하여 간섭이 발생하였음을 알 수 있다. 이 경우 재밍 신호로 인해 수신단에서 결합 기법을 수행하였을 때 BER이 3.3×10^{-2}이였다. 그러나 재밍이 없는 경우 BER은 약 10^{-8}로 재밍 공격으로 인한 BER 성능 저하가 큼을 알 수 있다. 본 실험에 대한 자세한 결과는 그림 12에 표시되어있다.

이러한 높은 BER 문제를 해결하기 위해 재밍 신호의 간섭 영향을 감소시키는 CFAR 검출 알고리즘을 적용한다. CFAR 검출기 설계 시 M_{tc}와 M_{gc}의 설정에 따라 임계 값이 변동하며 재밍 신호 검출에 영향을 끼친다. 본 논문에서는 식 (4-1)과 (4-2)에 사용된 M_{tc}와 M_{gc}는 각각 하나의 슬롯을 구성하는 심볼 수의 2배와 1배만큼 설정하였다.

그림 8은 그림 7과 동일한 상황에 대해 식 (8)로부터 계산되는 CA-CFAR, SO-CFAR의 임계 값을 이용

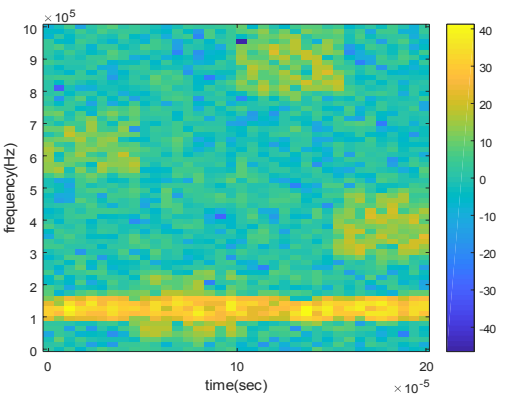


그림 7. FHSS 수신단 신호 spectrogram
Fig. 7. Spectrogram of the received signal for FHSS

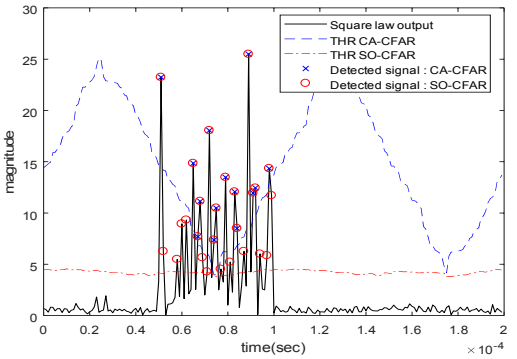


그림 8. CA-CFAR와 SO-CFAR를 이용하여 재밍 공격으로부터 간섭 영향을 받은 신호 검출
Fig. 8. Detection for the interfered signal by jamming attack by using CA-CFAR and SO-CFAR

해 재밍으로 인해 발생하는 간섭 신호를 검출한 예이다. 검은색 실선은 frequency de-hopping된 심볼인 $r_{dfh}(m)$를 square law detector를 통과시킨 결과로 $|r_{dfh}(m)|^2$ 이다. 파란색 파선과 빨간색 일점 쇄선은 각각 CA-CFAR와 SO-CFAR를 이용한 임계 값이며 파란색 십자 마커와 빨간색 원형 마커는 각각 CA-CFAR와 SO-CFAR로부터 검출된 간섭의 영향을 받은 신호이다. 이를 통해 간섭 영향을 받은 슬롯을 제거하고 부분 결합을 하였을 때 CA-CFAR의 BER은 1.1×10^{-4}, SO-CFAR의 BER은 2×10^{-5}이다. 본 실험에 대한 자세한 결과는 그림 12에 표시되어있다

그림 9와 그림 10은 $E_b/N_0=16$dB 경우에 ρ값이 각각 0.005, 0.05에 대하여 $P_{fa}=10^{-3}$, 10^{-4}, 10^{-5}, 10^{-6}으로 변화시키며 E_b/J_0의 변화에 따른

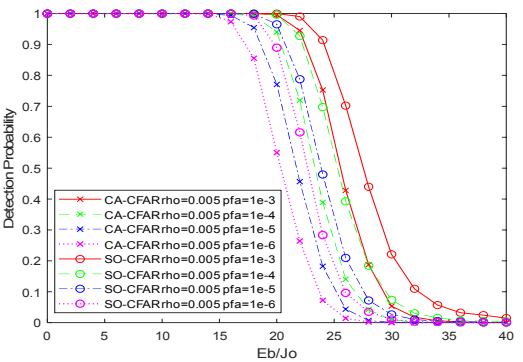


그림 9. $\rho=0.005$에서 CA-CFAR와 SO-CFAR를 이용한 간섭 슬롯 검출 확률
Fig. 9. Probability of the detection the interfered slot by using CA-CFAR and SO-CFAR in $\rho=0.005$

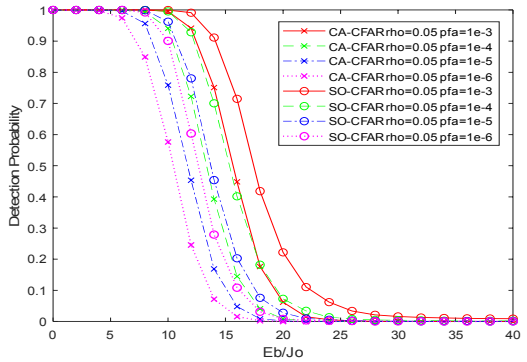


그림 10. $\rho=0.05$에서 CA-CFAR와 SO-CFAR를 이용한 간섭 슬롯 검출 확률
Fig. 10. Probability of the detection the interfered slot by using CA-CFAR and SO-CFAR in $\rho=0.05$

재밍 슬롯의 검출 성능을 나타낸 것이다. 빨간색 실선은 $P_{fa}=10^{-3}$ 초록색 파선은 $P_{fa}=10^{-4}$, 파란색 일점쇄선은 $P_{fa}=10^{-5}$ 그리고 보라색 점선은 $P_{fa}=10^{-6}$에 대한 것이고 십자 마커와 원형 마커는 각각 CA-CFAR와 SO-CFAR에 대한 검출 성능을 나타낸 것이다. E_b/J_0이 작은 경우는 간섭 영향을 받은 신호와 그렇지 않은 신호원 간의 레벨 차이가 크기 때문에 CA-CFAR과 SO-CFAR의 검출 성능은 100%이다. 그러나 E_b/J_0이 커짐에 따라 간섭 영향을 받은 신호와 그렇지 않은 신호간의 레벨차이가 크지 않기 때문에 재밍 검출 성능이 저하된다. 이때 SO-CFAR가 CA-CFAR에 비해 약 2dB 가량 검출 성능이 우수한 것을 알 수 있다. 그러나 E_b/J_0이 큰 경우에는 검출이 어렵기 때문에 SO-CFAR와 CA-CFAR의 검출성능이 유사해진다. 또한 같은 E_b/J_0에서 ρ에 따라 재밍 신호의 전력이 반비례하므로 작은 ρ인 경우 검출 성능이 우세함을 알 수 있다.

그림 11과 그림 12는 ρ값이 각각 0.005, 0.05에 대하여 기존의 전체 결합 기법, CA-CFAR와 SO-CFAR 검출을 통한 결합 기법의 BER 성능을 나타낸 것이다. 검은색 실선은 기존의 결합 기법이고 그 외의 범례는 그림 9와 동일하다. 재밍 검출이 완벽한 경우의 BER은 약 10^{-8}이다. E_b/J_0이 작은 경우에 기존의 결합 기법의 BER은 약 10^{-2}를 가지는 성능저하가 있지만 제안한 알고리즘의 경우 기존의 기법에 비해 우수한 성능을 갖는다. 그러나 E_b/J_0이 20

~25dB정도로 커지면 세 가지 기법의 BER 성능이 유사해진다. 이 이유는 그림 9, 10의 결과로부터 알 수 있듯이 E_b/J_0이 커짐에 따라 간섭의 영향을 받은

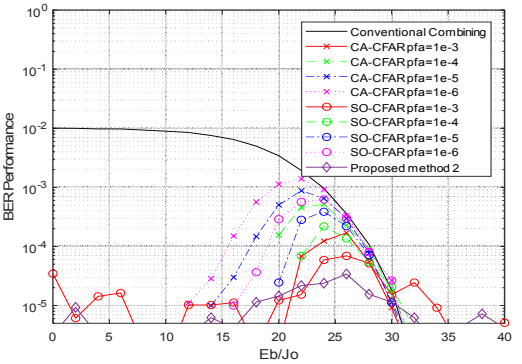


그림 11. $\rho=0.005$에 대한 BER 성능
Fig. 11. BER performance of $\rho=0.005$

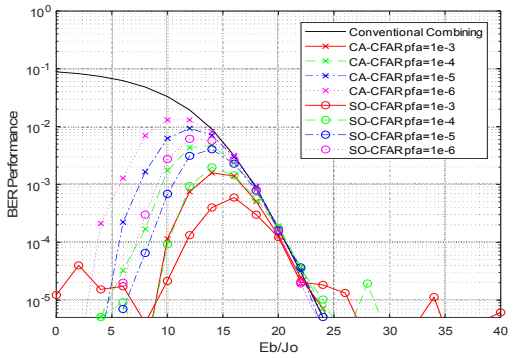


그림 12. $\rho=0.05$에 대한 BER 성능
Fig. 12. BER performance of $\rho=0.05$

신호와 그렇지 않은 신호들 간의 레벨차이가 작아지기 때문에 재밍 신호의 검출성능이 떨어지기 때문이다. 예를 들어, 그림 10에서 SO-CFAR의 P_{fa}가 10^{-3}인 경우 E_b/J_o이 10dB 부근에서 재밍 검출 확률이 급격하게 저하되는 것을 볼 수 있으며 그림 12의 동일 지점부터 검출이 안 된 재밍 신호 영향으로 BER 성능이 저하되는 것을 볼 수 있다. 이 후 결합하는 슬롯에 재밍이 존재하더라도 E_b/J_0이 커지면서 재밍 크기가 작아지기 다시 BER 성능이 향상된다. 이와 같이 재밍 검출 성능에 따라 BER 성능이 달라지고 재밍 검출 성능에 직접적인 영향을 주는 P_{fa}에 따라서도 BER이 변화하는 것을 알 수 있다. 즉, P_{fa}가 작은 경우 간섭 신호 검출 성능이 떨어지기 때문에 P_{fa}가 클 때에 비해 BER 성능이 저하된다. 그러나 P_{fa}가 10^{-3}이고 E_b/J_0가 30dB 넘는 경우에는 재밍 신호를 잘못 검출하여 결합 이득을 얻지 못하기 때문에 모든 슬롯을 결합한 BER 보다 성능이 저하되게 된다. 이처럼 P_{fa}에 따라 재밍 신호 검출 성능과 BER 성능의

trade-off 관계가 존재한다.

전산 모의실험 결과 본 논문에서 제안한 알고리즘이 기존의 결합 기법에 비해서 BER 성능이 우수하며 E_b/J_0과 ρ에 대하여 대체적으로 SO-CFAR 검출을 통한 결합 기법의 재밍 검출 성능과 BER 성능이 가장 우수함을 알 수 있다.

Ⅴ. 결 론

본 논문에서는 DQPSK 변조 방식을 이용한 같은 데이터를 반복적 슬롯으로 전송을 하는 FHSS 방식에서 협대역 잡음 재밍이 더해진 슬롯을 CA-CFAR와 SO-CFAR 기법을 통해 검출하여 제거한 후 나머지 슬롯을 결합하여 BER 성능을 향상시키는 알고리즘을 제안하였다. 전산 모의실험을 통해 기존의 결합 기법과 비교하여 제안된 방법을 사용할 경우 E_b/J_0이 10dB, $\rho=0.05$에서의 BER이 기존 3.3×10^{-2}에서 CA-CFAR을 이용 시 1.1×10^{-4} 그리고 SO-CFAR을 이용 시 2×10^{-5}로 성능 향상이 이루어짐을 보였다. 또한 $\rho=0.005, 0.05$과 $P_{fa}=10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}$에 대하여 E_b/J_0에 따른 BER 결과를 통해 SO-CFAR의 성능이 기존의 결합 기법과 CA-CFAR 기법에 비해 가장 우수함을 보였다.

References

[1] E. K. Lee, S. Y. Oh, and M. Gerla, “Randomized channel hopping scheme for anti-jamming communication,” in *Wireless Days(WD)*, Venice, Italy, 2010.

[2] J. H. Lee, J. H. Jang, J. E. Roh, K. J. Yoo, and J. H. Choi, “Jamming detection and suppression algorithm for an FMCW radar altimeter,” *J. KIEES*, vol. 27, no. 2, pp. 147-155, Feb. 2016.

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread spectrum communications handbook*, 2nd Ed., McGraw-Hill, 1994.

[4] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” *IEEE Commun. Surv. & Tuts.*, vol. 11, no. 4, pp. 42-56, Dec. 2009.

[5] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” in *Proc. IEEE Symp. Security Privacy*, pp. 64-78, Oakland, CA, USA, May 2008.

[6] Y. Liu, J. Hu, H. Wang, and D. Zhu, “A new anti-janiming method combining adaptive array antennas and frequency-hopping techniques,” in *Proc. ISCIT2005*, pp. 246-249, Beijing, China, Oct. 2005.

[7] F. J. Block and H. Nguyen, “Packet acquisition for low-complexity frequency-hop receivers,” in *Proc. MILCOM 2008*, San Diego, CA, USA, Nov. 2008.

[8] L. Simone, N. Salerno, and M. Maffei, “Frequency-hopping techniques for secure satellite TT&C: system analysis & trade-offs,” *2006 Int. Wksp. Satellite and Space Commun.*, pp. 13-17, Madrid, Spain, Sept. 2006.

[9] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks,” in *IEEE INFOCOM 2007*, pp. 2526-2530, Barcelona, Spain, May 2007.

[10] W. C. Park, K. C. Go, J. H. Kim, and K. K. Kim, “Anti-jamming method by using BER performance analysis of satellite communication system,” *J. KICS*, vol. 35, no. 10, pp. 1535-1543, Oct. 2010.

[11] B. Sklar, *Digital communications fundamentals and applications*, 2nd Ed., Prentice-Hall, Inc. 2001.

[12] Z. Messali, F. Soltani, and M. Sahmoudi, “Robust radar detection of CA, GO and SO CFAR in pearson measurements based on a non linear compression procedure for clutter reduction,” *J. Sign., Image Video Process.*, vol. 2, no. 2, pp. 169-176, Jun. 2008.

[13] J. Chung, E. J. Powers, W. M. Grady, and S. C. Bhatt, “Adaptive power-line disturbance detection scheme using a prediction error filter and a stop-and-go CA CFAR detector,” in *Proc. ICASSP 1999*, pp. 1533-1536, Phoenix, AZ, USA, Aug. 1999.

[14] G. V. Trunk, “Range resolution of targets using automatic detectors,” *IEEE Trans.*

Aerospace and Electron. Syst., vol. AES-14, no. 5, pp. 750-755, Sept. 1978.

[15] V. Hansen and J. Sawyers, "Detectability loss due to "Greatest of" selection in a cell-averaging CFAR," *IEEE Trans. Aerospace and Electron. Syst.*, vol. AES-16, no. 1, pp. 115-118, Jan. 1980.

[16] S. H. Mortazavi, M. A. Beach, J. A. Jones, and J. P. McGeehan, "Bit error simulation of DQPSK for a slow frequency hopping CDMA system in mobile radio communications," in *Proc. IEEE Symp. PIMRC 1995*, pp. 183-187, Toronto, Ont., Canada, Sept. 1995.

이 호 준 (Hojun Lee)

2016년 2월 : 인하대학교 전자공학과 학사 졸업

2016년 3월~현재 : 인하대학교 전자공학과 석사과정

<관심분야> 5G 통신, 신호 검출, machine learning

김 성 호 (Sungho Kim)

2000년 2월 : 경남대학교 전자공학과 학사 졸업

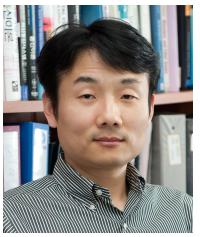
2002년 2월 : 경남대학교 전자공학과 석사 졸업

2002년 1월~2015년 9월 : 삼성탈레스 통신 연구소

2015년 9월~현재: 한화시스템 통신연구소 위성통신그룹

<관심분야> 이동통신, 위성통신 등

정 재 학 (Jaehak Chung)



1988월 2월 : 연세대학교 전자공학과 학사 졸업

1990년 2월 : 연세대학교 전자공학과 석사 졸업

2000년 : University of Texas at Austin 전기전산 학과 박사 졸업

2000년~2001년 : Post doctorial fellow, University of Texas at Austin

2001년~2005년 : 삼성종합기술원 수석연구원

2005년~현재 : 인하대학교 정교수

<관심분야> 5G 통신, 수중 통신, machine learning 등