

군 통신에서의 재밍(Jamming) 기술

김진영 | 김은철 | 이종명*

광운대학교, 명지대학교*

요 약

최근 전자전 (EW : Electronic Warfare)은 현대전의 핵심으로 자리매김하고 있다. 전자전에서 재밍 (Jamming)은 적군의 통신을 교란시키는 전자공격 (EA : Electronic Attack)을 의미하는 것으로 재밍 전술은 공격 대상에 따라서 여러 가지로 나눌 수 있다. 본고에서는 군통신에서 사용되는 전자방해책 (ECM : Electronic Counter Measure)인 재밍 기술을 소개하고, 재밍 신호에 대한 대책으로 재밍 신호를 효과적으로 검출하고 제거할 수 있는 전자방해방어책인 (ECCM : Electronic Counter Counter Measure) 항재밍 (Anti-Jamming) 방안도 함께 분석 소개하고자 한다.

I. 서 론

전자전 (EW : Electronic Warfare)이란 적이 사용하는 전자적 스펙트럼을 결정하고 역이용하며 무력화시키는 동시에 우군 전력을 보호하는 수단, 또는 적의 전자기 스펙트럼을 통제하기 위해 전자기 및 지향성 에너지를 사용하는 제반 군사 활동을 말한다. 따라서 전자전은 우군 혹은 적군이 방사하는 전자파를 이용하여 적의 전자무기체계 및 지휘통제 감시정찰(C4ISR : Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) 체계를 방해, 마비, 무력화 및 파괴하고, 적의 전자전 활동

및 전자기 간섭으로부터 아군의 전자파 사용을 보호하여 전자무기체계 및 C4ISR 체계의 효율적 운용을 보장한다 [1,2]. 이러한 전자전은 이라크전 및 걸프전에서 전쟁과 동시에 수행되어 이라크의 주요 지휘통제망을 마비시킴으로써 그 능력과 중요성이 입증되었다. 결국 전자전은 전쟁의 승패를 좌우할 정도로 현대전의 핵심이라고 말할 수 있다.

전자전의 전투 기법에는 전자지원책 (ESM : Electronic Support Measure), 전자방해책 (ECM : Electronic Counter Measure), 전자방해방어책 (ECCM : Electronic Counter Counter Measure) 등이 있으며, <표 1>에 설명되어 있다.

ECM은 여러 분류 방법이 있으나, 기술적으로 능동 ECM과 수동 ECM으로 분류할 수 있다.

능동 ECM에는 잡음 방해와 기만 방해가 있으며, 또한 수동 ECM에는 채프 (Chaff), 특수 반사체 등에 의한 기만 및 전파 흡수체를 이용한 스텔스 기술도 포함된다.

잡음 방해는 표적의 위치를 나타내는 신호의 주위를 강력한 방해 전파를 송신하는 방식이다.

기만 방해는 적의 레이더 등에 의해 허위 신호를 방사하여 자신의 위치를 오인시키는 것이다. 기만 방해의 특징은 다음과 같다. 우선, 기만 방해는 적은 에너지로 충분히 잡음 방해의 결과로 동등한 효과를 발휘할 수 있다는 점이다. 다음으로, 고밀도의 전파 환경에서도 능력을 최대로 발휘할 수 있다. 마지막으로 코히어런트 전파 신호를 재방사 할 수 있기 때문에 펄스 압축 레이더 등에 효과적이다. 기만 방해는 표적의 거리와 속도 및 방위각을 기만할 수 있다.

아주 가느다란 유리 섬유에 알루미늄을 얇게 입히거나, 나일론 섬유에 은을 도금한 것을 레이다 파장의 길이로 잘라

서 만든 한 다발의 실 뭉치를 공중에 뿌려 놓은 것이 채프이다.

ECCM은 적의 ECM으로부터 아군의 전자 시설을 보호하는 것으로서 우군에 관한 적의 첨보수집능력을 최소한으로 억제하는 대전자전 지원과, 우군의 전자장비가 방해 및 기만을 받을 때 피해를 최소로 줄이고 전자장비의 기능을 계속 최대로 유지하기 위한 대전자공격으로 구분된다.

본고에서는 전자전의 전술 중에서 적군의 통신을 교란시킴으로써 전투에서 유리한 위치를 차지하기 위한 전자공격 형태인 재밍 (Jamming) 기술 및 재밍 신호가 존재하는 상황에서도 신뢰성있는 통신을 하기 위한 대전자공격 형태인 항재밍 (Anti-Jamming) 방안을 소개하고자 한다.

〈표 1〉 전자 전투 (Electronic Combat) 기법

전자전투기법	내 용
전자지원책 (ESM)	<ul style="list-style-type: none"> 위협의 인지와 정보를 제공하기 위하여 방출된 전자파 에너지의 탐지와 위치 확인 및 식별을 하는 것 전자방해책 및 전자방해방어책을 지원하기 위한 전자전 정보를 제공 항공기 탑재 레이더 경보 수신기 (RWR : Radar Warning Receiver) 등
전자방해책 (ECM)	<ul style="list-style-type: none"> 적의 효과적인 전자파 스펙트럼 사용을 축소시키거나 방해하는 일련의 행동 잡음, 기만 재머, 통신 재머, 적외선 재머 등
전자방해방어책 (ECCM)	<ul style="list-style-type: none"> 송신기의 송신주파수 변경, 출력 증대, 필스 압축, 수신기의 수신이득 조절, 이동 타겟 지시기 (MTI : Moving Target Indicator) 등

II. 재 링

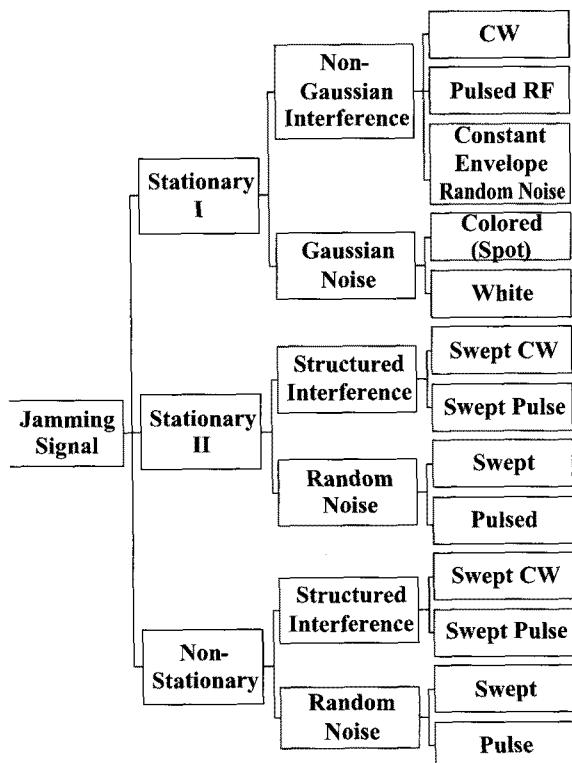
1. 개요

재밍이란 전자방해책으로 고전적 의미의 전자 공격이다. 이는 초고주파 (RF : Radio Frequency) 에너지를 방사함으로써 특정 주파수나 전파의 사용을 거부하도록 하는 교란 형태 또는 허위 정보를 전송하도록 하는 기만 형태로 행해진다.

ECM 초기의 재밍 목적은 적이 아군 항공기를 피격시키는데 필요한 일련의 절차들인 피격과정 (Kill-Chain)을 방해, 약화, 기만하는 것으로서 피격과정 요소들을 식별하여 그 취약점을 이용하는 것이다. 피격과정의 가장 취약한 부분은

보통 위험 체계에 따라 다르다. 피격과정 중 한 개의 요소만을 방해하는 것보다는 오히려 다수의 요소들을 방해하거나 약화시킴으로써 그 목적이 달성될 수 있다.

재밍에 사용되는 재밍 신호는 일반적으로 열잡음과 구별되는 특징 (Non-White Power Spectral Density, Non-Stationary, Non-Gaussian)을 가지고 있다. 재밍 신호는 Stationary 여부에 따라 'Stationary- I 재밍 신호', 'Stationary-II 재밍 신호', 'Non-Stationary 재밍 신호'의 세 가지로 분류할 수 있다. 먼저, Stationary- I 신호는 통계적 특성과 전력 스펙트럼 밀도 (PSD : Power Spectral Density) 가 상수로 일정한 재밍 신호이다. 다음으로, Stationary-II 신호는 통계적 특성과 전력 스펙트럼 밀도가 시간에 따라 변하지만, 일정 주기의 짧은 시간 동안은 상수로 일정한 재밍 신호이다. 마지막으로, Non-Stationary 신호는 통계적 특성과 전력 스펙트럼 밀도가 시간에 따라 변하는 재밍 신호이다. (그림 1)은 이러한 재밍 신호를 세분한 것이다.



(그림 1) 재밍 신호 분류

현대 차세대 ECM장비들은 적이 모르게 은밀히 작동하도록 설계된 최첨단 디지털 시스템들이며, 적의 위협 레이더를 통제하고 반응을 관리하는 능력을 갖추고 있다. 더욱 중요한 것은 위협체계의 성능 개선 사항을 분석하고 대응할 수 있는 종합적인 대응 능력을 갖고 있다는 점이다. 이러한 기술적 접근 방식은 적의 감지를 방해하는 기술에서 은밀한 기만과 유인 기술로 발전하게 되었다.

2. 재밍 종류

재밍은 <표 2>에 나타낸 바와 같이 공격 방법 및 공격 대상에 따라 여러 종류가 존재한다.

<표 2> 재밍 분류

구 分	종 류
공격 방법	협대역 재밍
	광대역 재밍
공격 대상	기무시안 재밍
	톤 재밍
	대역잡음 재밍
	펄스 재밍
	주파수 추적 재밍
	링크 계층 재밍
	네트워크 계층 재밍
	추적 차단기
	역이득 구형파 재밍

① 협대역 (Narrowband) 재밍

미리 정해진 하나 이상의 주파수 대역에 대한 재밍이다. 이 재밍은 고속 순차 (Fast Sequential) 재밍 방식으로 수행되는데, 미리 정해진 협대역 주파수들을 임의의 순서 또는 'Swept Jamming'이라 불리는 대역 형태의 연속적인 순서로 재밍을 가한다.

② 광대역 (Broadband) 재밍

이 재밍은 광대역 변조를 통해 모든 주파수 대역을 동시에 커버하는 임의의 중심주파수에 재밍을 가한다.

③ 가우시안 (Gaussian) 재밍

재밍 신호가 가우스성 잡음과 동일하게 간주되는 경우로

서, 재밍 신호 $J_{Gauss}(t)$ 는 잡음의 형태와 동일하게 식 (1)과 같이 표현할 수 있다.

$$J_{Gauss}(t) = \alpha \cos(\omega t - \theta) \quad (1)$$

여기서 α , ω , 및 θ 는 각각 가우시안 재밍 신호의 크기, 주파수 및 위상이다.

④ 톤 (Tone) 재밍

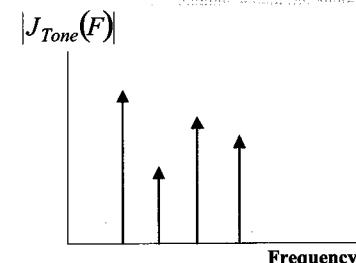
특정 주파수의 정현파는 주파수 축에서 하나의 톤으로 나타난다. 따라서 하나 또는 여려 개의 톤으로 이루어진 신호로 가하는 재밍을 톤 재밍이라 하고, 톤 재밍 신호 $J_{Tone}(t)$ 는 식 (2)와 같이 나타낼 수 있다 [3].

$$J_{Tone}(t) = \sum_{i=1}^K \alpha_i \cos(\omega_i t - \theta_i) \quad (2)$$

여기서 K 는 톤 개수이고, α_i 와 ω_i 및 θ_i 는 각각 i 번째 톤의 크기, 주파수 및 위상을 나타낸다. 톤의 개수에 따라 단일 톤 재밍과 다중 톤 재밍으로 나눌 수 있다.

정현파를 퓨리에 변환하면 식 (3)과 같이 표현할 수 있으므로, 톤 재밍 신호의 주파수 대역에서의 표현은 (그림 2)와 같다.

$$\cos 2\pi f_o t \Leftrightarrow [\delta(f - f_o) + \delta(f + f_o)] \quad (3)$$

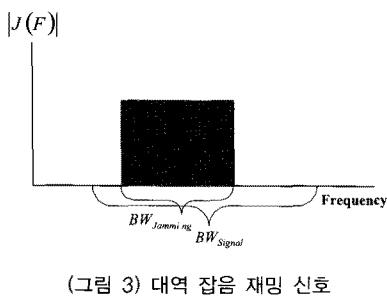


(그림 2) 톤 재밍 신호의 주파수 스펙트럼

⑤ 대역 잡음 (Band Noise) 재밍

대역 잡음 재밍은 주파수의 특정 대역에 걸쳐서 스펙트럼 밀도 N 를 갖는 신호를 이용해서 재밍하는 것이다. 공격 대상 신호의 대역폭 전체가 재밍 대역폭 내에 들어오는 경우

를 전대역 (Full-Band) 잡음 재밍이라 하고, 일부분만이 재밍되는 경우를 부분 대역 (Partial-Band) 잡음 재밍이라 한다. 대역 잡음 재밍은 주파수 도약 확산 스펙트럼 (FHSS : Frequency Hopping Spread Spectrum) 시스템에 효과적이다. 대역 잡음 재밍 신호를 주파수 대역에서 표현하면 (그림 3)과 같다.



(그림 3) 대역 잡음 재밍 신호

여기서 BW_{Signal} 은 신호의 대역폭이고, $BW_{Jamming}$ 은 재밍 신호의 대역폭이다. $\rho = \frac{BW_{Jamming}}{BW_{Signal}}$ 라고 하면, $\rho = 1$ 인 경우가 전대역 잡음 재밍이고, $0 < \rho < 1$ 인 경우가 부분 대역 잡음 재밍이다.

⑥ 펄스 (pulse) 재밍

펄스 재밍은 공격 대상 신호의 한 심볼 구간 내에서 일정 시간동안만 재밍 신호가 존재하는 경우를 말하고, 부분 시간 재밍이라고도 한다 [4]. 주파수 축에서 보면 전 대역에 걸쳐 재밍 신호가 존재하게 되므로, 대역 잡음 재밍의 한 종류로 분류할 수도 있다. 펄스 재밍은 직접 시퀀스 확산 스펙트럼 (DSSS : Direct Sequence Spread Spectrum) 시스템에 효과적이다.

⑦ 주파수 추적 (Frequency Follower) 재밍

주파수 추적 재밍은 광대역 수신기를 가지고 있어서, 공격 대상 신호의 주파수 대역을 모니터링하고 이에 맞춰서 재밍 신호를 발생시키는 것으로, 리피터 (Repeater) 재밍이라고도 한다. 이것은 반송파 주파수가 계속 바뀌는 주파수 도약 기법에 알맞은 재밍이다 [5,6].

직접 시퀀스 대역 확산 시스템은 확산 부호의 자기 상관 (Autocorrelation) 특성 때문에 일반적인 재밍은 효과적이지

못하다. 따라서 주파수 추적 재밍에서는 공격 대상 신호를 포착하여 잡음을 추가하거나 위상을 바꿔서 높은 전력으로 재전송함으로써, 수신기 입장에서 보면 시간적으로 지연된 송신 신호와 섞여서 효과적인 재밍이 가능하다 [7].

⑧ 링크 계층 (Link Layer) 재밍

톤, 대역, 펄스, 주파수 추적 재밍들은 물리 계층 재밍이며 링크 계층 정보가 없다. 링크 계층 재밍은 재밍을 하는 쪽에서 상위 계층의 정보를 알고 있는 경우 가하는 재밍으로서, 재밍 신호 낭비를 줄일 수 있다. 따라서 물리 계층 재밍에 비해서 전력 사용면에서 효율적인 재밍이다 [8,9]. IEEE 802.11 기반 MAC 프로토콜은 가상 반송파 감지 (Virtual Carrier Sensing) 기법을 사용한다 [10]. 따라서 대량의 허위 RTS/CTS (Request to Send/Clear to Send)를 전송해서 네트워크 사용률을 저하시키고, NAV (Network Allocation Vector)의 보류 시간을 길게 바꿔서 채널 낭비를 유도할 수 있다.

⑨ 네트워크 계층 (Network Layer) 재밍

무선 애드혹 (Ad-hoc) 네트워크는 유선 네트워크나 무선 네트워크에 비해 무선 채널 환경이 개방되어 있고, 동적인 네트워크 토플로지 (Dynamic Network Topology)를 가지며, 분산 협력 (Distributed Cooperation) 통신 구조이므로 안정성 (Security)에 취약한 특성을 가진다.

이와 같이 안정성에 취약한 무선 애드혹 네트워크의 특성을 이용한 재밍 기술이 네트워크 계층 재밍이다. 이는 데이터를 전송하기 위한 라우팅에 장애 요소를 유발시켜서, 정확하지 않은 라우팅 정보를 전파시키거나 제어 메시지 (Control Message Field)에 변형을 가하고, 각 노드의 라우팅 상태에 변형을 가한다.

패킷 전달에 대한 공격 (Packet Forwarding Attacks)으로는 데이터 패킷을 고의적으로 손실 시킴(Packet Dropping)으로써 대역폭, 메모리, 계산 능력과 같은 자원을 불필요하게 소비시키고 네트워크의 성능 저하 유발시킨다.

⑩ 추적 차단기 (RGPO : Range Gate Pull Off)

이는 허위 표적 신호를 이용하여 표적 반사 신호와 허위 표적 신호와의 시간차를 점차 증가 또는 감소시켜서 레이다 수신기가 큰 신호를 쫓아가도록 하는 방법이다. 결국 레이

다 수신기의 거리 계이트에는 허위 표적만 존재하게 되어 실제 표적을 놓치게 된다. 이를 RGWO (Range Gate Walk Off)라고도 하며, 기만 재밍 기법의 추적 차단 기법중 하나이다.

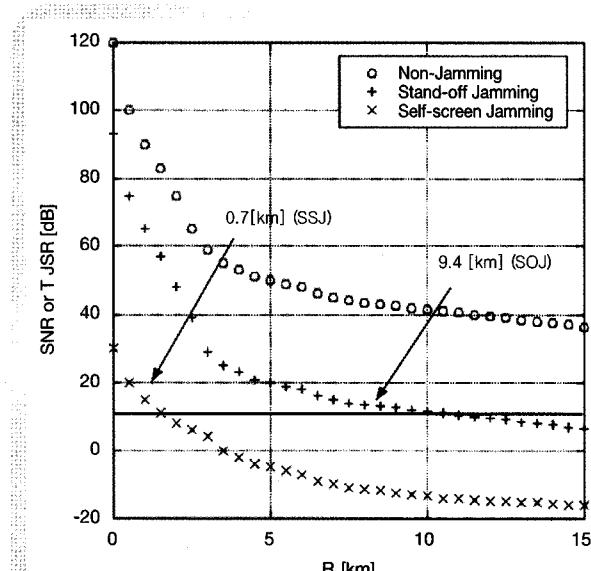
⑪ 역이득 (Inverse Gain) 구형파 재밍

역이득 구형파 재밍은 원뿔 주사 (Conical Scan) 레이다에 대한 각도 기만 재밍 기법으로 역 원뿔주사 (Inverse Conscan) 기법이라고도 한다. 레이다에 수신되는 펄스 포락선의 위상이 변경되거나 왜곡되면 레이다 스크린에서는 표적의 위치가 기반되어 여기저기에 표적이 존재하는 것처럼 나타나는데, 레이다의 이러한 특성을 이용한 재밍 기법이 역이득 구형파 재밍이다.

3. 재밍 성능

이번 절에서는 재밍 환경 하에서의 시스템 성능을 소개한다.

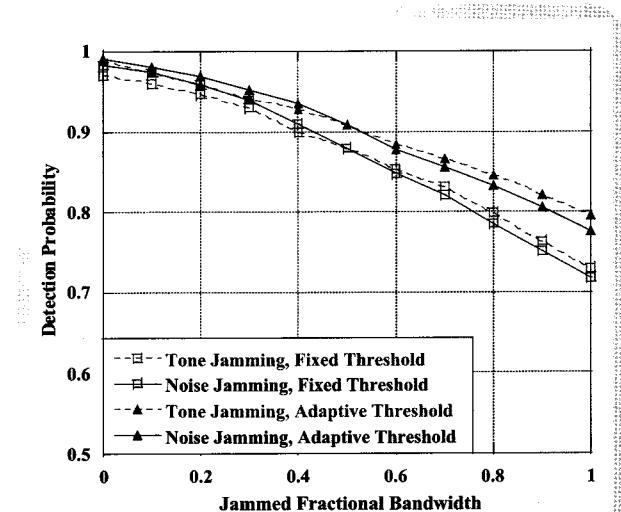
(그림 4)는 항공기 (RCS : Radar Cross Section = 4m^2)의 경우, 잡음 재밍 환경하에서 각 표적과의 거리에 따른 레이더의 SNR 분석 결과를 나타낸 것이다 [11]. 여기서 굵은 실선은 잡음 재밍 환경에서의 0.99의 탐지 확률을 위해 요구되는 $\text{SNR}_0 \approx 14.5\text{ dB}$ 가 되는 지점이다. 각각의 재밍 환경에 대한



(그림 4) 잡음 재밍 환경하에서 표적과의 거리에 따른 레이더의 SNR의 관계 ($\text{RCS}=4\text{m}^2$)

SNR을 살펴보면, 재밍 신호가 없는 환경 (NOJ : Non-Jamming)에서는 0.99의 탐지 확률을 위해 요구되는 SNR이 표적과의 거리가 15 km 이상일 때에도 유지되므로 15 km 이상에서도 표적의 탐지가 가능하다. SOJ (Stand-Off Jamming) 환경에서는 SNR이 14.5dB가 되는 지점은 표적과의 거리가 9.4km 일 때이므로, 9.4km 이상일 때에는 표적의 탐지가 곤란하다. SSJ (Self-Screen Jamming) 환경에서는 표적과의 거리가 0.7km 이내로 접근하지 않는 경우 표적의 탐지가 불가능하다.

[12]에서는 주파수 도약/대역확산 다중접속 (FH/SSMA : Frequency Hopping/Spread Spectrum Multiple Access) 시스템에서 부분 잡음 재밍과 톤 재밍 신호가 있는 경우에 대하여 적응적으로 임계치를 조절하여 포착 (Acquisition) 성능을 분석하였다. (그림 5)는 사용자가 10명이고 4개의 다중 경로가 존재하며 재밍 대 신호 전력 비 (JSR : Jamming to Signal Power Ratio)가 10 dB인 경우, 재밍된 대역 비율에 따른 검파 확률을 나타낸다. 실험 결과, 재밍된 대역 비율이 1로 가까워짐에 따라 검파 확률이 감소하는 것을 확인할 수 있다. 따라서 전 대역을 재밍하는 것이 최적의 재밍 전략이다.



(그림 5) 잡음과 톤 재밍 환경하에서 재밍된 대역 비율에 따른 검파 확률

III. 항재밍 방안

과거의 군통신 및 상용 통신 시스템은 DSSS 또는 FHSS 시스템이 주를 이루었기 때문에 항재밍 기법에 관한 연구는 대부분 이를 시스템을 기반으로 하는 것이었다 [13-16]. 이번 장에서는 항재밍 방안에 대하여 제시한다.

1. DSSS/FHSS

DSSS 및 FHSS 기법은 항재밍 성질을 보유하므로 20세기 초반부터 군 통신을 위한 용도로 연구되고 시스템이 개발되었다 [13,14]. SS 기법은 주파수 축에서 신호를 확산시켰다가 다시 역확산시키는 과정에서 잡음 및 간섭 신호를 제거하는 효과를 얻는다. DSSS 시스템은 대역 잡음 재밍에는 강하지만 펄스 재밍에 취약한 단점을 가지고, FHSS 시스템은 펄스 재밍에는 강하지만 부분 대역 잡음 재밍에는 취약한 성능을 보인다.

AWGN 채널 환경 하에서 펄스 재밍 신호가 존재하는 경우, DSSS 시스템의 BER 성능은 식 (4)와 같이 표현할 수 있다.

$$P_b = (1 - \rho) Q\left(\sqrt{\frac{2E_b}{N_o}}\right) + Q\left(\sqrt{\frac{2E_b}{N_o + J_o / \rho}}\right) \approx \rho Q\left(\sqrt{\frac{2E_b}{J_o / \rho}}\right) \quad (4)$$

여기서 $\rho = \begin{cases} 0.709 & \frac{E_b}{J_o} > 0.709 \\ \frac{E_b}{J_o} & 1 \\ 1 & \frac{E_b}{J_o} \leq 0.709 \end{cases}$ 이다. 따라서 DSSS 시스템에

재밍 신호가 존재하는 경우 BER 성능의 최대값은 식 (5)와 같이 표현할 수 있다.

$$P_{b,\max} = \begin{cases} \frac{0.083}{E_b / J_o} & \frac{E_b}{J_o} > 0.709 \\ Q\left(\sqrt{\frac{2E_b}{J_o}}\right) & \frac{E_b}{J_o} \leq 0.709 \end{cases} \quad (5)$$

AWGN 채널 환경 하에서 펄스 재밍 신호가 존재하는 경우 FHSS 시스템의 BER 성능은 식 (6)과 같이 표현할 수 있다.

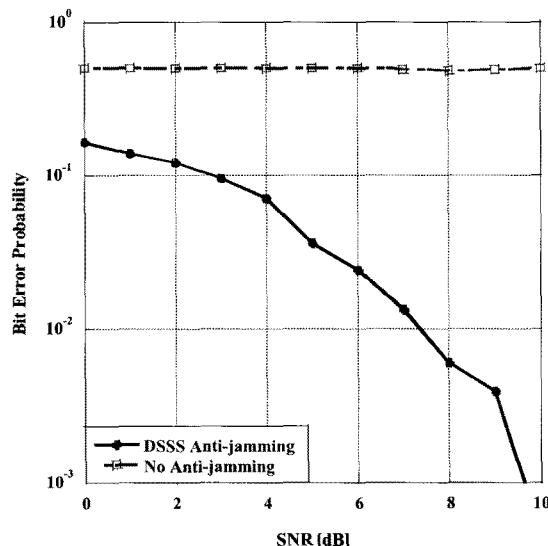
$$P_b \approx \frac{\rho}{2} \exp\left(-\frac{\rho E_b}{2 J_o}\right) \quad (6)$$

여기서 $\rho = \begin{cases} \frac{2}{E_b / J_o} & \frac{E_b}{J_o} > 2 \\ 1 & \frac{E_b}{J_o} \leq 2 \end{cases}$ 이다. 따라서 FHSS 시스템에

재밍 신호가 존재하는 경우 BER 성능의 최대값은 식 (7)과 같이 표현할 수 있다.

$$P_{b,\max} = \begin{cases} \frac{e^{-1}}{E_b / J_o} & \frac{E_b}{J_o} > 2 \\ \frac{1}{2} \exp\left(-\frac{E_b}{2 J_o}\right) & \frac{E_b}{J_o} \leq 2 \end{cases} \quad (7)$$

(그림 6)은 대역 잡음 재밍 신호가 원하는 신호와 동일 대역에 존재하는 경우, AWGN 채널에서 DSSS 시스템의 성능을 나타낸다. 성능 분석 결과 항재밍을 하지 않은 경우는 재밍 신호로 인해 수신기에서 원래 신호를 복구하지 못하는 반면에, DSSS 시스템은 대역 잡음 재밍에 대해서 항재밍 성능이 우수한 것을 확인할 수 있다.



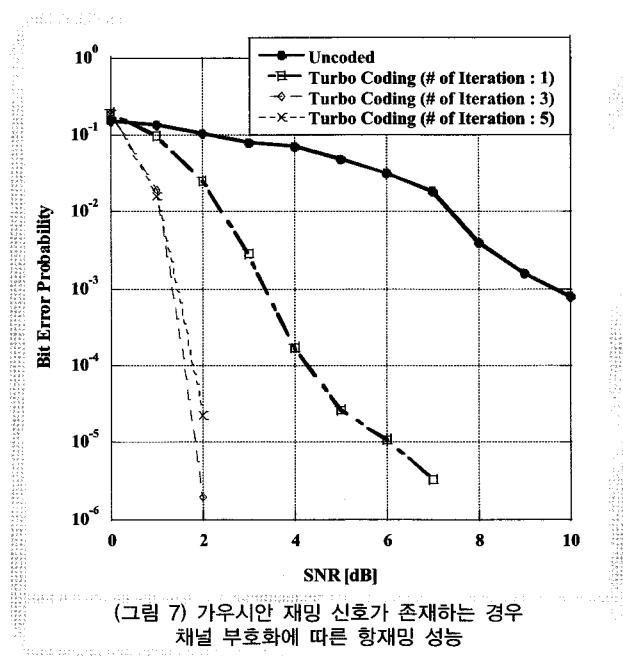
(그림 6) 대역 잡음 신호가 존재하는 경우 DSSS의 항재밍 성능

1. 채널 부호화 (Channel Coding)/인터리빙 (Interleaving)

채널 부호를 사용하지 않는 경우에는 재밍 신호에 의해 한

번 오류가 생기면 그대로 성능 열화로 이어지지만, 채널 부호를 사용하면 전송률에서 손해를 보는 대신 채널 부호의 오류 정정 능력 내에서는 재밍 신호에 의해 발생한 오류를 복구함으로써 성능 열화를 막을 수 있다 [13]. 또한 시간 또는 주파수 축에서 인터리빙을 함으로써, 부호어 (Codeword)의 특정 부분에 오류가 몰려서 발생하는 것을 방지하여 재밍 신호를 시간 또는 주파수 축에서 넓게 퍼뜨리는 것과 같은 효과를 얻을 수 있다 [16]. 하지만 채널 부호화와 인터리빙은 재밍 신호를 적극적으로 제거하지는 못하므로 항재밍 능력에 한계가 있다.

(그림 7)은 가우시안 재밍 신호가 존재하는 경우 채널 부호화에 따른 항재밍 성능의 실험 결과를 나타낸다. 이 때 채널 부호로 터보 부호를 선택하였으며, 반복 복호 회수에 따라 항재밍 성능을 실험하였다. 그림에서 확인할 수 있는 바와 같이 채널 부호를 이용하면 가우시안 재밍 신호가 존재하여도 재밍의 영향을 극복할 수 있는 것을 확인할 수 있다. 또한 수신기의 복호 과정에서 반복 복호 회수를 증가시키면 항재밍 성능이 증가하는 것을 확인할 수 있다.



3. 클리핑 (Clipping)/이레이징 (Erasing)

클리핑 또는 리미팅 (Limiting) 기법은 항재밍 기법 중에서 가장 간단하면서도 좋은 성능을 가진다 [17-19]. 클리핑은 단

순히 정해진 임계치를 넘는 신호를 강제적으로 임계치로 제한하는 기법이다. 이의 극한적인 형태로, 임계치를 넘는 신호를 결합 또는 복호 과정에서 제외시켜서 신뢰성이 떨어지는 정보를 이용하지 않는 것이 이레이징이다.

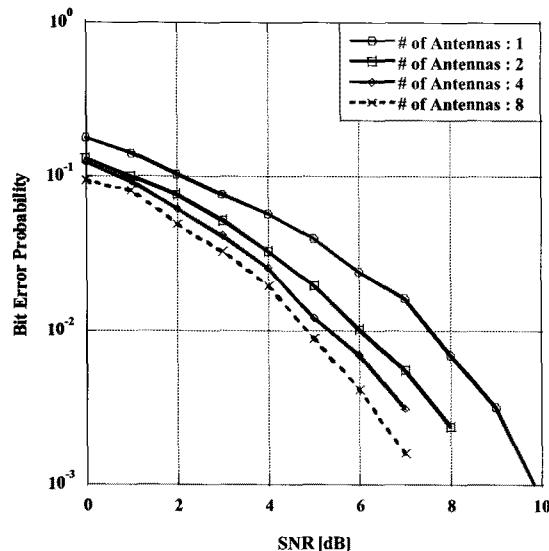
4. 필터링

클리핑과 이레이징은 재밍 신호에 대한 사전 정보가 거의 없어도 사용할 수 있으며, 간단하게 구현할 수 있는 장점이 있다. 하지만 재밍 신호에 대한 통계적인 정보를 알 수 있다면 이를 이용하는 필터링 기법을 통하여 항재밍 성능을 향상시킬 수 있다. 필터링은 수신 신호 성분 중에서 원하는 신호 성분은 통과시키고 그렇지 않은 신호 성분은 제거하는데 그 목적이 있다.

5. 다중 안테나 기법

지향성 안테나 (Directional Antenna)는 원하는 방향으로 신호의 세기를 증가시켜 송신하거나 특정한 방향으로부터 오는 신호를 잘 수신할 수 있도록 하는 기법으로서, 군사 통신 환경과 같은 무선 애드혹 네트워크에서 공간 재사용, 송신 전력 제어를 통하여 채널 용량과 신호 전달 범위를 향상시킬 수 있다. 이는 빔형성을 이용하여 백색 잡음 형태의 재밍을 방사하는 재머가 존재하는 환경에서 방향성 안테나에 적합한 프로토콜을 적용한 경우, 무지향성 안테나 (Omni Antenna)를 사용한 경우보다 재밍의 간섭을 줄이고 송신 전력을 효율적으로 사용함으로써 패킷 수신율을 높일 수 있다. 그리고 이러한 성능 차이는 재밍 전력이 커질수록 더욱 크게 나타난다 [20].

(그림 8)은 가우시안 재밍 신호가 존재하는 경우 다중 안테나 기법에 따른 항재밍 성능 실험 결과를 나타낸 것이다. 이 때 안테나 수는 1개, 2개, 4개, 8개인 경우에 대해서 실험하였다. 그림에서 확인할 수 있는 바와 같이 다중 안테나를 사용할 경우가 하나의 안테나를 사용하는 경우보다 항재밍 성능이 우수한 것을 확인할 수 있다. 또한 다중 안테나를 사용하는 경우 안테나 수가 증가할수록 항재밍 성능이 증가하는 것을 확인할 수 있다. 하지만 성능 증가폭은 감소하는 것을 확인할 수 있다.



(그림 8) 가우시안 재밍 신호가 존재하는 경우
다중 안테나 기법에 따른 항재밍 성능

IV. 결 론

본고에서는 전자전에서 사용되는 재밍 기술 및 재밍에 대한 대응책인 항재밍 방안에 대하여 분석 소개하였다. 재밍 기술은 공격 방법, 공격 대상 및 전자 에너지 사용 여부에 따라 여러 가지가 존재한다. 그리고 재밍 신호의 성질에 따라 여러 항재밍 기법이 적용될 수 있다.

차세대의 재밍 기술은 다양한 플랫폼의 무선 시스템들을 무력화 할 수 있는 첨단 기술로 여겨지고 있다. 이를 위해서는 기존의 재밍 방안들을 균형있게 통합 발전시켜야 한다. 단순한 전자방해책 보다는 탄력적이고, 신뢰성이 있으며, 비용 대비 효과가 우수한 전자방해책을 제공할 수 있는 방향으로 발전하여야 한다.

감사의 글

본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음.

(IITA-2008-C1090-0803-0002)

참 고 문 헌

- [1] 공군본부, 직무교육교본 항로통신 정비조수 및 기사: 제 1권, 2002.
- [2] 공군본부, 공교 0-2-5(15) 운용교리: 전자전, 2001.
- [3] L. B. Milstein, S. Davidovici, and D. L. Schilling, "The effect of multiple-tone interfering signals on a direct sequence spread spectrum communication system," *IEEE Trans. Commun.*, vol. 30, no. 3, pp. 436-446, Mar. 1982.
- [4] Q. Ling and T. Li, "Modeling and detection of hostile jamming in spread spectrum system," in *Proc. of SAFE*, pp. 1-5, Apr. 2007.
- [5] D. Torrieri, "Fundamental limitations on repeater jamming of frequency-hopping communications," *IEEE J. Select. Areas Commun.*, vol. 7, no. 4, pp. 569-575, May 1989.
- [6] A. A. Hassan, J. E. Hershey, and J. E. Schroeder, "On a follower tone-jammer countermeasure technique," *IEEE Trans. Commun.*, vol. 43, no. 2, pp. 754-756, Feb. 1995.
- [7] W. Hang, W. Zanji, and G. Jingbo, "Performance of DS-SS against repeater jamming," in *Proc. of ICECS*, pp. 858-861, Dec. 2006.
- [8] Y. W. Law, P. Harter, J. den Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC," in *Proc. of WSN*, pp. 217-225, Feb. 2005.
- [9] G. Thamilarasu, S. Mishra, and R. Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad-hoc networks," in *Proc. of MILCOM*, pp. 1-7, Oct. 2006.
- [10] IEEE 802.11, Part 11: *Wireless LAN Medium Access Control and Physical Layer Specifications*, Nov. 1997.
- [11] S. Kim and J. Kang, "A technique for the quantitative analysis of the noise jamming effect," *J. KIMST*, vol. 8, no. 4, pp. 91-101, Dec. 2005.
- [12] J. Y. Kim and J. H. Lee, "Acquisition performance with adaptive threshold for a FH/SSMA system," *IEICE*

- Trans. Commun.*, vol. 79, vo. 3, pp. 297-306, Mar. 1996.
- [13] T. Scholtz, "The spread spectrum concept," *IEEE Trans. Commun.*, vol. 25, pp. 748-755, Aug. 1977.
- [14] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread-spectrum communication-a tutorial," *IEEE Trans. Commun.*, vol. 30, pp. 855-884, May 1982.
- [15] L. B. Milstein, R. L. Pickholtz, and D. L. Schilling, "Optimization of the processing gain of an FSK-FH system," *IEEE Trans. Commun.*, vol. 28, pp. 1062-1079, Jul. 1980.
- [16] J. Proakis, "Interference suppression in spread spectrum systems," in *Proc. of ISSSTA*, vol. 1, pp. 259-266, Sep. 1996.
- [17] C. Baum and M. Pursley, "Erasure insertion in frequency-hop communications with fading and partial band interference," *IEEE Trans. Veh. Technol.*, vol. 46, no. 4, pp. 949-956, Nov. 1997.
- [18] A. Oppenheim and R. W. Schafer, *Discrete-Time Signal Processing*, Prentice-Hall, 1989.
- [19] T. Kasparis, M. Geroqipoulos, and E. Payne, "Non-linear filtering techniques for narrow-band interference rejection in direct sequence spread-spectrum systems," in *Proc. of MILCOM*, vol. 1, pp. 360-364, Nov. 1991.
- [20] Z. Zhang, B. Ryu, G. Nallamothu, and Z. Huang, "Performance of all-directional transmission and reception algorithms in wireless ad-hoc networks with directional antennas," in *Proc. of MILCOM*, vol. 1, pp. 255-260, Oct. 2005.

약력



김진영

1998년 서울대학교 전자공학과 학부학사

1998년 ~ 2000년 미국 Princeton University Research Associate

2000년 ~ 2001년 SK텔레콤 네트워크연구원 책임연구원

2009년 ~ 2010년 미국 MIT 공대 Visiting Scientist

2011년 ~ 현재 광운대학교 전파공학과 부교수

관심분야: 디지털 통신, 무선통신, 체널 부호화



김은철

2003년 광운대학교 전자공학부 공학사

2005년 광운대학교 전파공학과 공학석사

2005년 ~ 현재 광운대학교 전파공학과 공학박사과정

관심분야: 무선통신, 체널 부호화, 양립성



이종영

1976년 서울대학교 전자공학과 학부학사

1978년 서울대학교 전자공학과 공학석사

1987년 North Carolina State University, ECE Dept.(Ph.D.)

1978년 ~ 1997년 국방과학연구소 책임연구원

1997년 ~ 1999년 테이콤 연구소 부소장

1999년 ~ 2005년 하나로텔레콤 CTO(부사장)

2006년 ~ 현재 명지대학교 통신공학과 교수

관심분야: Military Communications, Fault Tolerant System,

Ad-hoc, Data Link, Convergence

