부채널화를 통한 효율적인 부분대역 재밍 회피 알고리즘과 성능분석

송유찬*, 황유민*, 박지호*, 김진영*, 신요안**

Performance Analysis of Efficient Subchannelization Algorithm against Partial Band Jamming

Yu Chan Song*, Yu Min Hwang*, Ji Ho Park*, Jin Young Kim*, and Yoan Shin**

요 약

최근 전자전은 현대전의 핵심으로 자리매김하고 있으며 미래 전투체계인 네트워크 중심전에 따른 통신 생존의 중요성은 나날이 부각되고 있다. 본 논문에서는 GPS 재밍 등 군통신에서 사용되는 전자 방해책인 재밍 기술을 효과적으로 제거할 수 있는 항재밍 방안에 대해 제안하기 위해 부분대역 재밍 환경과 군통신에 널리 사용되는 IEEE 802.16 WiMAX 프로토콜을 고려하였다. 기존의 주파수 도약 방법과는 다른 부채널화를 통한 알고리즘을 제안하였으며, 제안한 알고리즘의 성능 확인을 위해 부분대역 재밍 파라미터에 따른 최대 채널용량에 해당하는 최대 부채널 개수를 확인할 수 있었다.

Key Words : Dynamic frequency selection, frequency hopping, partial band jamming, subchannelization, channel capacity.

ABSTRACT

Electronic warfare recently has became the core of modern warfare and the importance of communication survivability is being considerable day by day. In this paper, we propose an effective jamming avoidance algorithm aginst widely used jamming environment such as GPS jamming. In order to simulate to show our system performance, we consider IEEE 802.16 WiMAX protocol and partial band jamming envoriment. Proposed algorithm can improve channel capacity through subchannelization and we show channel capacity corresponding to subchannel parameter.

I. 서 론

미래 전투체계인 네트워크 중심전으로의 전장 환경변화로 인해 무인전투체계와 그에 해당하는 통신의 생존성은 더욱 중요해지고 있다. 전장에 투입되는 전자장비들은 적군의 재밍 공격에 노출되기 쉽기 때문에 재밍으로 인해 발생하는 정보의 손실을 막기 위한 항재밍은 필수적이다. 정해진 프로토콜에 따라 동작하는 것을 악의적으로 방해하는 재밍은 계층 및 공격 대상에 따라 여러 유형으로 나누어 볼 수 있다. IEEE 802.16은 일반적인 무선통신 네트워크와 마찬가지로 재밍과 서비스거부(Denial-of-Service:DOS) 공격에 약하다 [1]. 통신에 의도적으로 문제를 발생시키는 공격자는 기지국의 특정 주파수에 지속적이거나 간헐적인 재밍 공격을 가해 네트워크를 마비시키는 공격 유형이다. 다양한 유형의 재밍 공격을 탐지할 수 있는 기법으로서 Carrier-to-Interference-plus-Noise-Ratio(CINR)를 이용하는 방법 등이 연구되고 있으나, 본 논문에서는 재밍 탐지 기법을 별도로 다루지 않으며 기지국과 단말(User Equipment: UE)은 즉각적인 재밍 공격을 탐지할 수 있다고 가정한다.

무선 네트워크에서 재밍 공격에 대한 효과적인 대처 방안으로 채널 도약이 알려져 있다. 채널 도약 수행 시 재밍 공격 상황에서도 약간의 성능 저하가 있지만 여전히 네트워크 운용이 가능하다. 본래 IEEE 802.16 표준은 주파수 도약 스펙트럼 확산을 정의하고 있다. 채널 도약은 일정 시간 간격으로 채널 도약을 수행하는 능동적 도약 (proactive hopping)과 채널 상태의 변화 등에 의해 도약을 수행하는 대응적 도약 (reactive hopping)으로 나누어 볼 수 있다. 대표적인 방

※이 논문은 2014년도 국방과학연구소 핵심기술연구개발 과제의 지원을 받아 수행되었음 (UD140076ED).
*광운대학교 유비쿼터스 통신 연구실 (yuchan@kw.ac.kr, yumin@kw.ac.kr, jihopark@kw.ac.kr, jinyoung@kw.ac.kr)
**숭실대학교 통신및정보처리 연구실 (yashin@ssu.ac.kr)
접수일자 : 2015년 4월 17일, 수정완료일자 : 2015년 4월 25일, 최종게재확정일자 : 2015년 5월 2일

법 중 하나인 Dynamic Frequency Selection(DFS) 기법은 각 채널 상태를 측정한 후 사용 여부와 재밍유무를 확인하여 최적의 채널을 선택한다. 기존의 DFS는 재밍 공격 발생 시 새로운 채널을 탐색하는 Full DFS Test 구간에 의해 재머 대응에 일정한 시간이 걸리며 그 시간 동안 통신이 두절되는 단점을 가지고 있다. 또한 새로운 도약채널의 선택은 전채널을 검사한 후에 이루어지므로 채널 간의 도약 시간과 전체 채널 개수에 비례하여 재머에 대응하기 위한 시간이 늘어나게 된다.

본 논문에서는 IEEE 802.16 WiMAX 표준 프로토콜에 따라 작동하는 무인전투체계를 가정하며 부분재밍공격(partial band jamming)이 발생할 때 재밍 공격에 노출된 인접채널을 제외한 사용 가능한 모든 채널을 최대한 사용함으로써 기존의 주파수도약 방법과는 다른 부채널화 알고리즘를 통해 시스템 성능을 개선하였다. 시뮬레이션을 통해 부분대역 재밍 파라미터에 따라 최대의 채널용량을 갖는 부채널의 개수와 최대채널용량을 확인할 수 있었다.

Ⅱ. 시스템 모델

재밍은 상대방의 통신 체계를 혼란시키거나 방해하는 행위이며 광대역 재밍, 부분대역 재밍, 톤 재밍, 가우시안 재밍, 협대역 재밍 등 공격 방법 및 공격 대상에 따라 여러 종류가 존재한다. 평균전력이 제한된 재머는 제한된 부분주파수대역에 집중적으로 재밍신호를 발생시키는 것이 더욱 효과적인 방법이다. 따라서, 본 연구에서는 부채널을 사용하는 802.16 WiMAX시스템에서 부분대역 재밍이 있는 환경을 고려하였다. 부분대역 재밍은 대역폭이 광대역 재밍보다 작은 것을 제외하고는 같은 가우시안 특성을 가진다.

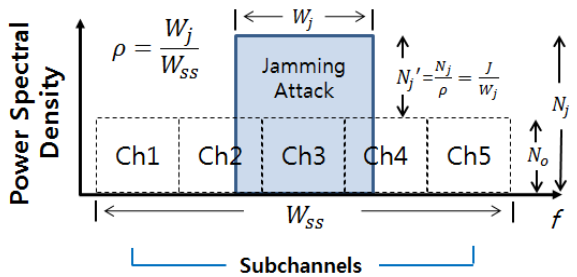

그림 1. 부분대역 재밍 모델.

그림 1은 배경잡음과 부분대역 재밍이 동시에 존재하는 경우의 재밍 모델을 도식화하였다. 5개의 부채널이 존재하며 3번채널을 사용 중일 때 3번채널과 인접채널인 2번,4번 채널이 부분대역 재밍 공격을 받게 되는 예시이다. N_0는 AWGN의 전력밀도함수(power spectral density function)이고 고의적인 재밍신호의 전력밀도함수는 N_j로 정의한다. 또한, W_{ss}는 전주파수대역, W_j는 재밍주파수대역, J는 재밍신호전력, N_j는 재밍신호의 전력밀도함수, ρ는 재밍신호의 대역점유율을 나타낸다. 부분대역 재밍에서 잡음전력 J는 전체 확산대역 W_{ss} 중 일부분인 W_j 대역에 분포할 때 전체확산 대역 중 잡음의 분포 비율은 ρ로 나타내며 다음과 같이 나타낼 수 있다.

$$\rho = \frac{\omega_j}{\omega_{ss}}, \tag{1}$$

부분대역 재밍의 경우 ρ의 값은 0보다 크고 1보다 작은 값을 갖게 된다.

그림 2와 3은 부분대역 재밍 공격에 대한 회피 알고리즘 작동 방식을 나타낸다. 기지국의 초기동작은 기지국과 단말 간에 할당된 전채널을 사용한다. 채널에 대한 정보를 단말에 전달하여 정상작동하여 데이터를 송수신 하며, 재밍 공격 탐지가 된 이후에는 부분 재밍 탐지 및 회피를 위해 기지국과 단말에 할당된 900MHz~920MHz 주파수 대역의 20MHz에 대한 부채널을 형성하고 채널 측정을 통해 각 채널의 재밍 공격에 대한 영향 유무를 확인하여 가용 채널을 확보한다. 재밍 공격을 받는 채널을 제외하여 사용 가능한 채널을 선택 후 선택된 채널의 정보를 단말에 송신하여 기지국과 단말 사이의 정상적인 통신이 이루어지게 된다. 채널탐색 구간은 비콘을 통해 각 채널에 대한 측정을 수행하는 것을 말하며, 모든 단말이 데이터 전송을 중지하는 구간이다. 제안하는 기법은 비콘을 통해 현재 채널을 포함한 전체 채널의 상태를 측정한다.

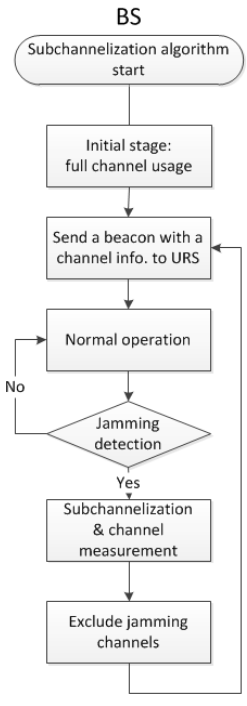

그림 2. 제안하는 알고리즘(기지국).

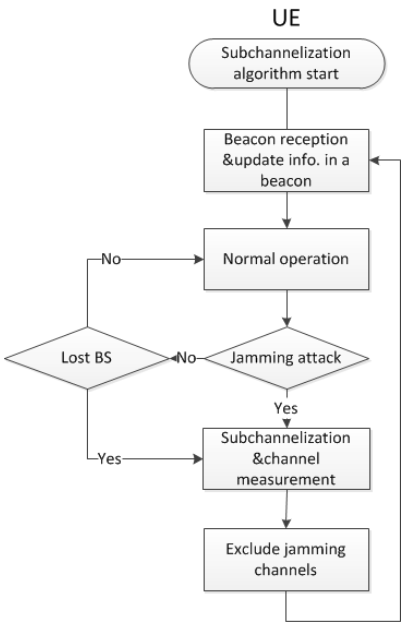

그림 3. 제안하는 알고리즘(단말).

단말(UE)은 기지국(BS)에 의해 할당된 채널정보를 비콘을 통해 수신하여 할당된 채널을 사용하여 정상적인 통신을 하게 된다. 재밍 공격 발생 시 재밍에 영향을 받는 채널을 제외한 가용채널을 탐지하며, 재밍 공격 탐지 혹은 기지국과의 통신 품질 저하 문제가 발생할 때 부채널화 및 채널 측정을 시행하게 된다.

Ⅲ. 부채널화를 통한 부분대역 재밍 회피 성능 분석

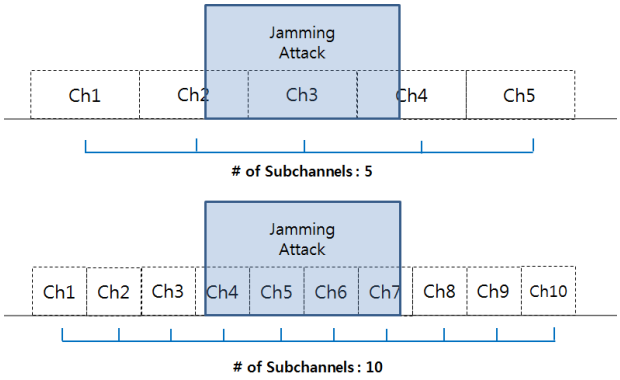

그림4. 부채널 개수 증가에 따른 주파수대역 효율 증가.

그림4는 부분대역 재밍 공격이 발생할 때 부채널화를 통한 재밍 대응 방식에 관련된 그림을 도식화 한 것이다. 부채널의 개수가 5개일 때, 부분대역 재밍에 영향을 받지 않는 사용 가능한 채널은 Ch1, Ch5이다. 부채널의 개수가 10개일 때, 부분대역 재밍에 영향을 받지 않는 사용 가능한 채널은 Ch1, Ch2, Ch3, Ch8, Ch9, Ch10으로 부채널의 개수가 5개일 때 보다 더 넓은 주파수대역을 사용할 수 있어 보다 효율적인 재밍 회피 방안이 확실하다. 성능분석을 위한 채널용량의 식은 다음과 같다.

$$C = W\log_2(1+\frac{\overline{P_r}}{N_0 W}), \quad (2)$$

$\overline{P_r}$[W]은 평균수신파워, N_0[W/Hz]는 노이즈 파워스펙트럼밀도, W는 대역폭을 나타내며, $\frac{\overline{P_r}}{N_0 W}$는 SNR을 나타낸다.

채널 측정을 위한 단계에서는 모든 단말이 전송을 중지하는 구간이므로 현재 채널을 적어도 현재 네트워크의 간섭 없이 측정할 수 있다.

Ⅳ. 모의실험

표 1. 파라메터 설명.

Parameter	값
Jamming time	50msec
Jamming detection time	5msec
number of subchannels	10,20,30
Channel model	AWGN channel
Carrier frequency	900MHz
Effective channel bandwidth	20MHz
Channel capacity (without jamming)	2Mbps
BS Tx power	13dBm
Noise power	-122dBm
Power distribution	Equal power distribution over all subchannels
Constellation	BPSK

제안하는 알고리즘의 성능 분석을 위해 설정된 파라메터는 표 1과 같다. 재머 탐지 시간은 재머가 현재 채널의 사용 여부를 다시 검사하는 시간이다. 시뮬레이션 단계에서 IEEE 802.16 WiMAX 시스템을 적용하였는데, 이는 국내의 무인로봇 통신 시스템 연구개발에 mobile WiMAX 기반 통신기술을 적용함으로써 링크비율의 가변적 적용을 통해 보다 유연한 통신환경의 구축이 가능하고 오류정정 성능이 뛰어난 Convolutional Turbo Code(CTC) 기술을 적용하여 강인한 무선링크 성능을 보장할 수 있어 차후 무인로봇체계 운용개념에 맞추어 효과적으로 적용할 수 있는 환경을 고려하였다.

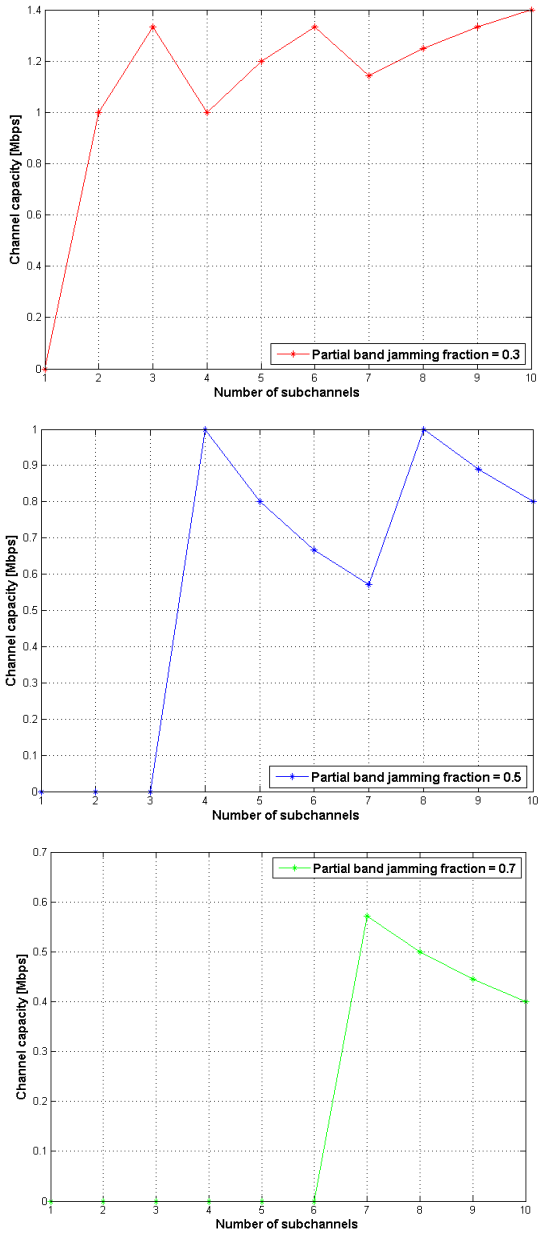

그림 5. 부채널 개수에 따른 채널용량(ρ=0.3, 0.5, 0.7).

본 논문에서 제안한 부분대역 재밍 회피 알고리즘의 성능을 확인하기 위한 시뮬레이션 결과는 그림 5와 같다. 부분대역 재밍 파라미터인 ρ(0.3, 0.5, 0.7)에 따라 실험을 진행하였으며 결과는 다음과 같다. ρ=0.3, 0.5, 0.7 일 때, 각각 부채널의 개수가 10개, 4개, 7개일 때 1.4Mbps, 1Mbps, 0.571Mbps로 최대용량을 갖는 것을 확인할 수 있었다. 똑같은 채널용량일 때 부채널의 개수가 적을수록 우수한 시스템이라고 할 수 있다. 이는 부채널의 개수가 증가할수록 채널측정에 소요되는 시간이 커지고 채널측정 기간에는 기지국과 단말 사이에 데이터 전송이 중지되기 때문이다.

Ⅴ. 결론 및 향후 연구 방향

본 논문에서는 기존의 주파수도약 기법과는 다른 재밍회피 기법인 부채널화 알고리즘을 제안하였다. 제안하는 부분대역 재밍 공격에 대한 회피 알고리즘은 재밍 공격 이전에는 단말간에 할당된 전채널을 사용 중에 있다가 재밍 공격 탐지 이후에 적용된다. 재밍 공격 탐지 이후에는 기지국과 단말에 할당된 주파수 대역에 부채널을 형성하며 채널 측정을 통해 각 채널의 재밍 공격에 대한 영향 유무를 확인하여 가용채널을 확보한다. 사용 가능한 채널을 판단한 이후에는 선택된 채널의 정보를 단말에 송신하여 기지국과 단말 사이에 통신이 이루어지게 된다. 시뮬레이션을 통해 부분대역 재밍 파라미터인 ρ에 따른 채널용량을 확인할 수 있었다. 한편, 본 논문에서 가정한 부분대역 재밍 환경 이외에 다양한 재밍 환경과 운용환경을 고려하여 재밍에 대응할 수 있는 높은 데이터 송수신 효율을 갖는 알고리즘의 연구 및 개발이 필요하다.

참 고 문 헌

[1] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, “Analysis of mobile WiMAX security: Vulnerabilities and solutions,” in Proc. of IEEE 5th Int. Conf. Mobile Ad Hoc Sensor Syst., pp. 1270-1212, Sept. 2009.

[2] L. Milstein, S. Davidovici, and D. Schilling, “The effect of multiple-tone interfering signals on a direct sequence spread specptrum communciation system,” IEEE Trans. Commun., vol. 30, no. 3, pp. 436-446, Mar. 1982.

[3] P. Dent, G. E. Bottomley, and T. Croft, “Jakes’ fading model revisited,” Elect. Lett., vol. 29, no. 3, pp. 1162-1163, June 1993.

[4] S. De Fina, “Comparison of FH-MA communications using OFDM and DS-MA systems for wideband radio access,” in Proc. of ICUPC’98, vol. 1, pp. 143-147, Oct. 1998.

[5] T. Shigehiko, R. Mino, S. Hara, and Y. Hara, “Performance comparison of OFDM-FH and MC-CDM in single- and multi-cell environments,”in Proc. of VTC’05, vol. 3, pp. 1730-1734, May-June 2005.

[6] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks,” in Proc. of INFOCOM’07, pp. 2526-2530, 2007.

[7] A. Mishra, V. Shrivastava, D. Agarwal, S. Banerjee, S. Ganguly, “Distributed channel management in uncoordinated wireless environments,” in Proc. of MOBICOM., pp. 170-181, Sept. 2006.

저자

송 유 찬(Yu Chan Song) **준회원**

- 2014년 2월 : 광운대학교 전파공학과 졸업
- 2014년 3월 ~ 현재 : 광운대학교 전파공학과 석박통합과정

<관심분야> : 4G 이동통신, 가시광통신, D2D, LBS, 빅데이터.

황 유 민(Yu Min Hwang) **준회원**

- 2012년 2월 : 광운대학교 전파공학과 학사
- 2012년 3월 ~ 현재 : 광운대학교 전파공학과 석박통합과정

<관심분야> : 4G 이동통신, 디지털 통신, 가시광통신, D2D, LBS, 인지무선통신.

박 지 호(Ji Ho Park) **준회원**

- 2014년 2월 : 광운대학교 전자융합공학과 졸업
- 2014년 3월 ~ 현재 : 광운대학교 전파공학과 석사과정

<관심분야> : 무선 에너지 하비스팅, LBS, 협력통신

김 진 영(Jin Young Kim) **종신회원**

- 1998년 2월 : 서울대학교 전자공학과 공학박사
- 2001년 2월 : SK텔레콤 네트웍 연구소 책임연구원
- 2001년 3월 ~ 현재 : 광운대학교 전자융합공학과 교수

<관심분야> : 다지털통신, 가시광통신, UWB, 부호화, 인지무선통신, 4G 이동통신

신 요 안(Yoan Shin)

- 1992년 12월 : Univ. of Texas at Austin 전기 및 컴퓨터공학과 공학박사
- 1994년 9월 ~ 현재 : 숭실대학교 전자정보공학부 교수
- 2008년 1월 ~ 2008년 12월 : 한국통신학회 이동통신연구회 위원장

<관심분야> : 이동 및 무선통신, 통신신호처리