논문 15-40-11-11 The Journal of Korean Institute of Communications and Information Sciences '15-11 Vol.40 No.11
http://dx.doi.org/10.7840/kics.2015.40.11.2188

# 전술 무선랜 재밍 환경에서의 형평성 성능 향상을 위한 채널도약 기법

김 용 철◆

# Channel-Hopping Scheme for Enhancing Fairness Performance under Smart Jammer Attacks in Tactical WLANs

Yongchul Kim◆

요 약

전술 무선랜 환경에서의 재밍 공격은 연속적인 전자기파를 발생시킴으로서 손쉽게 구현이 가능하며 주파수가 일치할 경우 그 피해는 매우 심각해질 수 있다. 무선 채널 환경은 누구나 공유할 수 있기 때문에 재밍 공격에 대한 완벽한 해결방법은 존재할 수 없으나 그 피해를 줄일 수 있는 방법으로 잘 알려진 기법이 채널도약 기법이다. 본 논문에서는 기존에 제안된 채널도약 기법들에 관하여 노드들의 데이터 전송용량과 노드들간의 형평성 측면에서 비교 분석하여 문제점들을 도출한 후 전술 무선랜 재밍 환경에 적합한 새로운 채널도약 기법을 제안한다. 또한 재밍 환경에서의 데이터 전송용량을 계산할 수 있는 분석 모델을 제안하여 채널도약 기법 적용시 규준화된 네트워크 데이터 전송용량을 쉽게 계산 할 수 있도록 하였다. 분석 모델을 이용한 수치 결과들은 제안된 채널도약 기법 적용시 규준화된 네트워크 데이터 전송용량은 다소 감소하지만 노드들간의 형평성 문제는 큰 폭으로 향상됨을 보여준다.

**Key Words** : Channel Hopping Scheme, Jamming Attacks, WLAN

ABSTRACT

In tactical wireless local area networks, jamming attack can easily occur by sending out continuous radio signals. The damage will be serious when the channel frequency is identical. Since wireless channel environment is open to everyone, the perfect solution for jamming attack does not exist. However, a channel-hopping scheme is well known for mitigating those jamming attacks. In this paper, I consider various channel-hopping schemes in order to analyze the throughput and fairness performance under smart jammer attack. Also an analytical model is introduced to evaluate the throughput performances of channel-hopping schemes. After analyzing well known channel-hopping schemes, I propose a simple channel-hopping scheme that can enhance fairness significantly at minimal throughput degradation expense.

## Ⅰ. 서 론

휴대용 컴퓨터와 스마트폰의 사용이 급격하게 증가함에 따라 무선 통신 기술중 근거리 통신망을 위한 표준기술로서 가장 널리 사용되는 기술이 IEEE 802.11 WLAN이다. WLAN은 기본적으로 인터넷에 데이터를 전달해 주는 기능을 하는 무선접속장치(AP)와 노트북이나 스마트폰과 같이 사용자가 서비스를 받는

※ 본 논문은 육군사관학교 화랑대연구소의 2015년도 연구활동비 지원을 받아 연구되었음(20150507).
◆ First Author : Korea Military Academy, Department of Electrical Engineering, kyc6454@kma.ac.kr, 종신회원
논문번호 : KICS2015-06-187, Received June 16, 2015; Revised August 10, 2015; Accepted October 21, 2015

단말간의 통신을 지원하는 기술로서 최근에는 군 통신 환경에서도 많이 이용되고 있다. 특히 군 전술 작전 본부(TOC:Tactical Operations Centers) 내에서의 통신에 많이 활용되고 있으며 미군에서도 TOC 통신을 지원하기 위하여 IEEE 802.11 기술을 바탕으로 SWLAN(Secure Wireless Local Area Network)[1] 시스템을 구축하여 활용중에 있다. SWLAN은 동기화 기술과 안테나 다이버시티 기술, 순방향 오류 정정 기술(FEC)등을 강화하여 보다 정확하고 더 멀리 통신할 수 있도록 개선된 기술로서 네트워크 중심전(NCW:Network Centric Warfare)의 안전한 C4I 시스템을 구축하기 위한 핵심 기술중에 하나로 인식되고 있다. 그러나 이러한 SWLAN 시스템도 재밍(Jamming) 공격에 대해서는 완벽하게 방어를 할 수 없는 것이 현실이다. 즉, 스마트한 재머(Jammer)들은 채널을 스캔하여 사용 중인 채널을 찾아낼 수 있는 능력을 가지고 있으며 채널이 탐지되었을 때 임의의 패킷들을 연속적으로 전송하여 정상적인 데이터 전송을 방해할 수 있기 때문이다. 그밖에 다양한 방법으로 재밍을 실시하는 재머들의 종류에 대하여는 Xu[2], Sufyan[3] 등이 제시한 논문을 참고한다.

재밍 공격의 피해를 줄이기 위한 방법에 관한 연구는 최근까지 활발하게 이루어지고 있으며 가장 대표적인 방법이 채널도약 기법(Channel hopping Scheme)을 사용하는 것이다. Navda[4] 등은 재밍 공격시 802.11 무선랜의 저항능력을 향상시키기 위해 채널도약 기법을 적용하는 방안에 대하여 소개 하였고, Jeung[5] 등은 재밍 공격을 감지한 경우 임의의 채널을 선택하지 않고 전체 채널 측정을 통해 가장 좋은 채널로 도약하는 측정기반 채널도약 기법을 제안하였으며, Lee[6] 등은 다양한 재밍 공격 환경에서 적용 가능한 랜덤 채널도약 기법(Randomized Channel Hopping Scheme)을 제안하기도 하였다.

채널도약 기법은 크게 두 가지 종류로 나누어 볼 수 있다. 첫째는 능동적(Proactive) 채널도약 방식[7]으로 재머의 존재나 채널의 상태에 상관없이 일정 시간 간격으로 네트워크내의 모든 노드들이 채널을 도약하는 방식으로서 재머들의 공격이 잦은 상황에서는 효과적인 방법이지만 재머의 공격이 없는 상황에서는 불필요한 채널 도약으로 인하여 채널 사용 효율을 떨어뜨리는 방식이다. 두 번째는 대응적(Reactive) 채널도약 방식[8]으로 채널 상태가 변화하였을 때 채널 도약을 실시하고 그렇지 않은 경우는 채널 도약을 실시하지 않는 방식이다. 재밍 공격이 없거나 채널 상태가 양호할 경우 불필요한 채널 도약을 방지하여 채널 사용 효율을 증가시킬 수 있으나 한 채널을 장시간 사용하므로 스마트 재머들로부터 쉽게 사용중인 채널이 탐지 되어 재밍 당할 수 있는 방식이기도 하다. Khattab[9] 등은 다양한 재머 공격 상황에서 능동적 채널도약 방식과 대응적 채널도약 방식을 비교 분석하였으며 멀티 라디오(Multi-radio) 네트워크 환경에서 대응적 도약 방식이 좀 더 재밍 공격에 대한 저항 능력이 우수함을 보이기도 하였다. 본 논문에서는 능동적 채널도약 방식을 적용하여 재머 공격에 대응하는 상황을 가정하였으며 특히 스마트 재머 공격시 능동적 채널도약 방식의 성능을 구체적으로 분석하고자 한다. 또한 유사한 환경을 고려하여 최근에 제안된 채널도약 기법으로 Jeung[10] 등이 제안한 deception mechanism을 소개하고 그 효과를 구체적으로 분석하여 문제점을 도출한 후 군 전술 무선랜 재밍 환경에 적합한 새로운 채널도약 기법을 제안하고자 한다.

스마트한 재머들의 공격 상황에서 피해를 최소화하기 위해 제안된 능동적 채널도약 방식에서의 deception mechanism은 스마트 재머에 의해 채널을 탐지 당하였을 때 재밍 당한 노드를 제외한 나머지 노드들로 하여금 정해진 채널도약 시간까지 기다리지 않고 재밍 공격을 감지하였을 때 즉시 채널 도약을 실시하여 네트워크의 전체적인 데이터 전송용량을 향상시키는 기법이다. 재밍을 당한 노드는 계속해서 스마트 재머를 유인하기위해 채널 도약을 실시하지 않고 같은 채널에 남아 있는 것이 큰 특징인데 이는 소수를 희생하여 다수를 만족시키는 대표적인 방법이라 할 수 있다.

그러나 군 전술통신 환경에서와 같이 단 하나의 노드만 재밍을 당한다 하더라도 전체적인 작전에 치명적인 영향을 미칠 수 있는 상황에서는 위와 같은 방법은 바람직하지 않으며, 또한 대부분 군사 목적의 재머들은 단 하나의 노드만을 목표로 삼고 공격하기도 하기 때문에 새로운 방법으로 대응해야 한다. 이에 본 논문에서는 스마트한 재머들의 공격상황에서 어느 특정 노드만 희생하지 않고 모든 노드들이 공평하게 전송용량을 달성할 수 있는 채널도약 기법을 제안하여 형평성 성능을 향상 시키고자 한다.

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 능동적 채널도약 방식에서의 사용자 노드와 스마트 재머 모델을 제시하고 형평성 성능 향상을 위한 새로운 채널도약 기법을 제안하였으며, Ⅲ장에서는 재밍 환경에서의 규준화된 네트워크 데이터 전송용량을 계산할 수 있는 수치 분석 모델을 제시하였다. Ⅳ장에서는 제안된 채널도약 기법 적용 시 수치해석 결과를 통

해 노드들 간의 형평성 성능이 향상됨을 보였으며, V 장에서 결론을 맺는다.

## Ⅱ. 형평성 성능 향상을 위한 채널도약 기법

본 논문은 스마트한 재머들의 공격 상황에 대응할 수 있는 능동적 채널도약 방식을 가정하여 기본적으로 일정한 시간 간격으로 모든 노드들이 채널을 도약하게 된다. 이때 한 채널에 머무르는 시간을 DT(dwell time)라 하고 다음 채널로 도약하는데 걸리는 시간을 ST(switching time) 라고 한다. 즉, 채널 상태에 관계없이 DT 마다 모든 노드들은 정해진 다음 채널로 도약해야 하고 도약 할 때마다 ST가 소요된다. ST는 항상 일정한 시간이지만 DT는 재머들의 공격 정도에 따라 변화 시켜 적용할 수 있는 시간이며 DT의 변화에 따라 네트워크 전체 데이터 전송용량에도 직접적인 영향을 미친다. 그림 1은 본 논문에 사용된 노드와 스마트 재머의 모델을 나타낸 것으로 DT와 ST를 비롯하여 재머가 한 개의 채널을 스캔할 때 걸리는 시간인 FT(finding time)와 재머가 채널을 찾아낸 이후 재밍하는 시간인 JT(jamming time)가 잘 나타나 있다. 이때 ST에 걸리는 시간을 t초라고 가정한다면 DT에 걸리는 시간을 상대적인 값인 $\alpha$t로 표현하여 $\alpha$를 DT slot이라고 정의하였다. 스마트 재머는 네트워크에 존재하는 노드들의 DT와 ST 간격을 알고 있지만 노드들의 채널 도약 순서를 알 수 없으므로 네트워크에서 사용되는 모든 채널을 스캔하여 사용중인 채널을 찾아내야 한다. 재머가 한 개의 채널을 스캔할 때 FT의 시간이 소요되지만 다음 채널을 스캔하기 위해 채널을 도약해야 하므로 그림 1에서 보는바와 같이 FT와 FT사이에 ST의 시간이 추가로 소요된다. 재머가 채널 k를 탐지하는데 성공하였다면 탐지된 순간으로부터 DT가 끝날때까지 계속해서 재밍을 실시할 수 도 있지만 좀 더 스마트한 재머는 JT 동안만 재밍을 실시하고 그 이후에는 채널이 여전히 사용되고 있는지 다시 확인하는 과정을 거쳐 채널을 사용하는 노드들이 감지되면 또다시 JT 동안 재밍을 실시하고 그렇지 않으면 다른 채널로 이동하여 다시 채널을 스캔하는 과정을 거치게 된다. [10]에서 제안된 deception mechanism은 이러한 스마트 재머의 특성을 잘 이용한 채널도약 기법으로서 채널이 스마트 재머로부터 감지가 되었을 때 실시간으로 패킷을 전송 중이던 한 개의 노드를 제외하고 나머지 노드들은 즉시 다음 채널로 도약하고 전송 중이던 노드는 계속 채널에 남아 스마트 재머가 JT 이후에 채널을 다시 확인할 때 계속해서 채널이 사용되고 있음을 인지하도록 재머를 속이는 기법이다. 이와 같은 기법은 동일한 네트워크에 다수의 사용자 노드들이 존재할 때 한 개의 노드만 희생시켜 다수의 노드들이 재머의 영향으로부터 피해를 최소화 할 수 있는 방법으로 상당히 효과적인 방법이라 할 수 있다. 그러나 희생당한 노드의 피해는 매우 치명적이며 이는 네트워크내의 사용자 노드들간의 불공평성 문제를 야기 시키게 된다. 특히, 군 전술통신 환경에서는 단 한 개의 노드라도 전송하고자 하는 데이터의 중요성이 매우 클 수 있으며 재머들의 목표가 다수의 노드들이 아닌 단 하나의 노드일 수도 있으므로 deception mechanism은 이러한 상황에서는 적절한 방법이 아니다.

본 논문에서는 군 전술통신 환경에서 사용가능한 채널도약 기법으로 스마트 재머로 부터의 피해를 최소화하고 특정 사용자 노드에게 재밍이 집중되는 현상을 방지할 수 있는 새로운 채널도약 기법을 제안한다. 스마트 재머가 채널을 탐지하여 재밍을 시작하면 재밍을 당하고 있는 노드가 JT 이후에 재머를 유인하기 위해 채널에 남아 있지 않고 바로 다음 채널로 도약을 하는 기법으로서 재밍을 당하지 않은 노드들 보다 채널 도약이 조금 느릴 수 있지만 재밍을 인지하였을 때 바로 다음 채널로 도약함으로써 그 피해를 최소화 할 수 있는 기법이다. 능동적 채널도약 방식이 적용된 상황에서 deception mechanism이나 새롭게 제안된 기법을 적용하지 않는다면 모든 사용자 노드들이 재밍 공격시 정해진 채널도약 시간까지, 즉 사용중인 채널의 DT 구간이 끝날 때까지 대기할 수밖에 없으며 그 피해는 DT 구간이 길어질수록 클 수밖에 없다. 그러나 deception mechanism은 재밍 당하고 있는 하나의 노드를 희생하여 사용 중인 채널의 DT 구간이 종료될 때까지 재머를 유인하고 나머지 노드들은 DT 구간 종료이전에 다음 채널로의 도약을 허용함으로써 데이터 전송용량을 향상시킨 기법이며, 새롭게

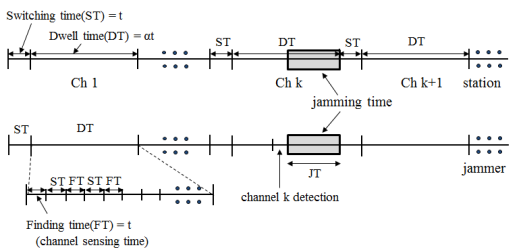


그림 1. 사용자 노드의 채널도약 모델과 스마트 재머의 채널탐지 모델
Fig. 1. Channel hopping model of user nodes and channel finding model of smart jammer

제안된 기법은 재밍을 당하고 있는 노드까지도 JT 이후 즉시 다음 채널로 도약을 허용하는 방법으로서 사용 중인 채널의 DT 구간이 끝날 때까지 대기해야 하는 능동적 채널도약 방식보다는 데이터 전송용량을 향상시킬 수 있는 방법이며 동시에 사용자 노드들 간의 형평성 성능을 향상시킬 수 있는 방법이다. 그러나 스마트 재머 또한 JT 이후에 채널에 사용 중인 노드가 없음을 인지하고 다시 채널 스캔을 실시하게 되므로 deception mechanism에 비하여 네트워크 전체 데이터 전송용량은 다소 감소될 수 있다. 그러므로 새롭게 제안된 기법의 성능을 능동적 채널도약 방식과 deception mechanism에 비교하여 구체적으로 분석할 수 있도록 다음 장에서 수치 분석 모델들을 제시하고자 한다.

## Ⅲ. 수치 분석 모델

본 논문에서 제안된 채널도약 기법의 성능을 분석하기 위하여 기존에 제안되었던 deception mechanism과의 비교 분석을 실시하고 DT와 JT의 변화에 따른 성능을 비롯하여 네트워크내의 사용자 노드 수에 따른 성능 변화를 구체적으로 살펴보고자 한다. 먼저 재머가 존재하지 않을때의 규준화된 네트워크 데이터 전송용량은 다음과 같이 표현된다.

$$Th_1 = \frac{DT}{ST+DT} \tag{1}$$

채널 도약을 위한 Switching time을 제외한 DT 전체 시간을 데이터 전송에 사용할 수 있으므로 높은 전송용량을 달성할 수 있다. 그러나 DT 구간이 짧아 채널 도약을 자주 실시해야 한다면 재머가 존재하지 않아도 전송용량은 감소하게 될 것이다. 스마트 재머가 존재하는 상황에서는 DT 구간이 짧으면 채널이 감지될 확률이 줄어들고 DT 구간이 길면 채널이 감지되어 재밍을 당할 확률이 커진다. 재머가 DT 구간 안에서 한 개의 채널을 스캔할 때 소요되는 시간이 FT+ST 이므로 DT 구간이 끝나기 전에 재머가 스캔할 수 있는 채널의 수를 N 이라고 한다면 다음과 같이 계산된다.

$$N = \frac{DT}{FT+ST} \tag{2}$$

네트워크 내의 노드들이 사용가능한 전체 채널의 수를 L 이라고 한다면 스마트 재머가 DT 구간 안에서 n(1, 2, ..., N)번째 채널을 스캔할 때 채널이 탐지될 확률은 $p_n = 1/L$ 이다. 그러므로 DT 구간 안에서 스마트 재머로부터 재밍을 당하는 평균 시간은 다음과 같이 표현된다.

$$E(t) = \sum_{n=1}^{N} (DT - nFT - (n-1)ST) \times p_n \tag{3}$$

그러므로 스마트 재머가 존재하는 상황에서 재밍 공격시 DT 구간이 끝나기 전까지 채널 도약을 허용하지 않는 전통적인 능동적 채널도약 방식에서의 규준화된 네트워크 데이터 전송용량은 다음과 같다.

$$Th_2 = \frac{DT - E(t)}{ST+DT} \tag{4}$$

스마트한 재머들의 공격 상황에서 피해를 최소화하기위해 제안된 deception mechanism은 스마트 재머에 의해 채널을 탐지 당하였을 때 재밍당한 노드는 스마트 재머를 유인하여 계속해서 DT 구간이 끝날 때까지 채널이 사용되고 있음을 속이기 위해 채널에 남아 있고 나머지 노드들은 채널 도약을 실시하여 다음 채널로 이동함으로써 네트워크의 전체적인 전송용량을 향상시키는 기법이다. 이때 재밍 공격을 감지하고 노드들에게 채널 도약을 알리며 다음 채널로 도약하는데 걸리는 총 시간을 그림 2에 표시된 것과 같이 HT 라 하고, 재머가 n번째 채널을 스캔할 때 채널이 탐지되어 재밍을 당한 노드가 DT 구간 안에서 실질적으로 사용이 가능한 구간을 $\sigma_n$이라고 하였다 ($\sigma_n = nFT + (n-1)ST$). 또한 재밍 공격이 시작된 이후에 채널 도약으로 인해 재밍당한 노드를 제외한 나머지 노드들이 추가로 사용 가능해진 구간을 $\lambda_n$이라고 하면 재머가 재밍을 하는 동안 채널 도약한 노드들이 DT 구간 안에서 사용가능한 총 구간은 $\sigma_n + \lambda_n$으로서 DT-HT와 같다. 그러므로 네트워크에 존재하는 총 노드들의 수를 M이라고 한다면, deception mechanism을 적용하였을 때 규준화된 네

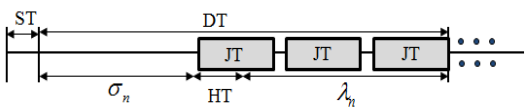


그림 2. 스마트 재머가 채널 탐지시 재밍 공격 방법
Fig. 2. Jamming attack method when a smart jammer detected a channel

트워크 데이터 전송용량은 다음과 같이 표현된다.

만약, 네트워크에 존재하는 노드들의 수가 많다면 한 개의 노드를 희생하여 다수의 노드들이 전송용량을 높일 수 있으므로 전체적인 네트워크 전송용량을 향상시킬 수 있는 방법이지만 반대로 네트워크에 존재하는 노드들의 수가 적은 경우에는 그 효과가 크게 줄어들게 되는 기법이다. 이를 구체적으로 분석하기 위해 네트워크에 존재하는 노드들의 수를 변화시켜가며 deception mechanism 기법을 적용한 결과 규준화된 네트워크 데이터 전송용량이 그림 3과 같이 나타났다.

극단적인 경우로 네트워트에 단 하나의 노드만 존재하는 경우에는 deception mechanism의 효과가 전혀 없음을 알 수 있으며, 노드의 수가 3 또는 10으로 증가할 때에 비로서 전송용량이 증가함을 알 수 있다. 그러나 전송용량의 증가는 네트워크에 존재하는 노드들의 증가분에 비례하는 것은 아니며 점차적으로 증가분이 감소하여 일정 수준에 수렴하게 된다. 시뮬레이션 결과 노드의 수를 50까지 증가시켜 보아도 그림 3의 10개 노드일때의 결과와 유사함을 알 수 있었다. 또한 재머가 없는 이상적인 경우의 전송용량과 비교해 보면 아무리 다수의 노드들이 채널도약으로 재머의 공격을 피한다 하더라도 단 하나의 노드가 재밍을 당함으로서 10% 이상의 성능 손실은 불가피 함을 알 수 있다. 이처럼 deception mechanism은 재밍을 당하는 노드 하나의 피해가 지배적이며 피해가 적은 나머지 노드들과의 형평성 문제가 심각하다. 이를 극복하기 위하여 본 논문에서 제안하는 기법은 재밍을 당하는 노드 또한 스마트 재머를 유인하기 보다는 재밍을 인지한 순간 즉시 다음 채널로 도약을 실시하여 나머지 노드들과 동일하게 재밍의 피해를 최소화 할 수 있는 기법이다. 그리하여 노드들간의 달성가능한 전송용량은 큰 차이가 없어 형평성 문제는 해결될 수 있으나 스마트 재머 역시 DT구간 내에서 첫 번째 JT이후에

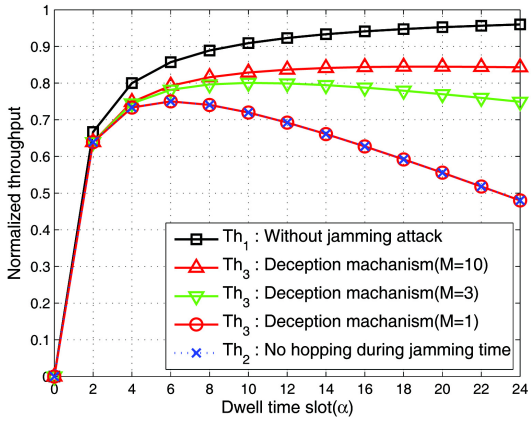


그림 3. 노드 수 변화에 따른 규준화된 네트워크 데이터 전송용량
Fig. 3. Normalized network data throughput with varying number of nodes(M)

채널에 존재하는 사용자 노드들이 없음을 인지하고 다시 채널 스캔을 실시하게 되므로 전체적인 네트워크 데이터 전송용량은 다소 감소될 수 있다. 제안된 기법에서 재밍을 당한 사용자 노드의 규준화된 전송용량을 표현하면 다음과 같다.

식(6)과 함께 재밍을 당하지 않은 사용자 노드들의 달성가능한 전송용량까지 고려하면, 제안된 기법의 규준화된 네트워크 데이터 전송용량은 다음과 같이 표현될 수 있다.

## Ⅳ. 수치 분석 결과

제안된 채널도약 기법의 성능을 분석하기 위하여 DT구간을 변화시켜감에 따라 달성가능한 규준화된 네트워크 전송용량을 측정해 보았다. 이때 노드들이 사용가능한 전체 채널의 수 L은 12개로 가정하고 ST와 FT에 걸리는 시간은 $t = 5ms$ 와 같다고 가정하였다. 그러므로 DT 구간의 기본 단위 슬롯 $\alpha$의 최대 값은 스마트 재머가 12개의 채널을 모두 스캔할 수 있

$$Th_3 = \frac{1}{M}\left( \frac{\sum_{n=1}^{N}\sigma_n p_n + \frac{DT(L-N)}{L}}{ST+DT} + \frac{\frac{(DT-HT)N}{L} + \frac{DT(L-N)}{L}}{ST+DT}(M-1) \right) \tag{5}$$

$$Th_j = \left( \sum_{n=1}^{N} \frac{\sigma_n}{ST+\min(\sigma_n+JT, DT)} \right) \frac{1}{L} + \frac{DT}{ST+DT}\frac{L-N}{L}, \tag{6}$$

$$Th_4 = \frac{Th_j + (Th_j + JT - HT)\times(M-1)}{M} \tag{7}$$

는 시간인 $12(FT+ST)=24t$와 같다. 또한, $M=3$ 이고 $HT=2t, JT=3t$ 라고 가정할 때 위에서 언급된 채널도약 기법들의 전송용량 결과들은 그림 4과 같다. 재머가 존재하지 않을때의 규준화된 네트워크 데이터 전송용량을 나타내는 $Th_1$은 DT구간이 길어질수록 전송용량이 증가하여 1에 가까워짐을 알 수 있다. 그러나 재머가 존재하여 재밍 공격을 받을 경우의 달성가능한 전송용량을 나타내는 $Th_2$는 DT구간이 길어질수록 그 피해가 더 심각해짐을 알 수 있다. 특히 DT구간 슬롯 $\alpha=24$일 때 규준화된 네트워크 데이터 전송용량은 약 0.5이며 이는 재머가 없을 때의 전송용량과 비교하여 대략 50% 정도 밖에 되지 않는 수준임을 알 수 있다. 이러한 전송용량의 피해를 최소화하기 위해 제안된 deception mechanism을 적용하였을 때의 전송용량인 $Th_3$는 DT구간이 길어질수록 다소 감소하기는 하나 $Th_2$에 비하여 큰 폭으로 향상되었음을 알 수 있다. 본 논문에서 제안된 채널도약 기법의 결과인 $Th_4$는 $Th_3$와 비교하여 DT 슬롯 $\alpha$값이 6이상일 때부터 규준화된 전송용량 값이 다소 작지만 전체적으로 매우 유사한 결과를 보여주었다.

Deception mechanism과 제안된 채널도약 기법의 형평성 측면에서의 성능을 비교 분석하기 위해서는 각각의 기법이 적용되었을 때 네트워크내에 존재하는 사용자 노드들의 데이터 전송용량을 비교해 보아야 한다. 즉, 재밍 공격을 당한 사용자 노드와 그렇지 않은 사용자 노드간의 데이터 전송용량을 비교하여 그 차이가 현저하게 크다면 형평성 측면에서 바람직하지 못한 결과라고 할 수 있다. 재밍 공격을 당한 사용자 노드가 달성가능한 데이터 전송용량이 해당 네트워크 내에서 가장 작은 값을 갖게 되므로 이때의 전송용량 값을 Minimum throughput 이라 하고 재밍 공격을 당하지 않은 사용자 노드의 데이터 전송용량을 Maximum throughput 이라고 하였을 때, 사용자 노드 수를 고려한 네트워크 평균 데이터 전송용량값을 Average throughput 이라고 할 수 있다. Deception mechanism과 제안된 채널도약 기법을 각각 적용하였을때 DT구간의 변화에 따른 사용자 노드들의 Maximum throughput 및 Minimum throughput을 그림 5와 그림 6에 각각 나타내었다. 그림 5에서 보듯이 deception mechanism에서는 재밍 공격을 받은 노드의 전송용량이 공격을 받지 않은 노드와 비교하여 현저하게 낮으며 DT 슬롯 $\alpha$값이 24일때는 최소 전송용량이 최대 전송용량의 55% 정도밖에 되지 않음을 알 수 있다. 반면에 그림 6에서 보듯이 본 논문에서 제안된 채널도약 기법을 적용하였을 때에는 재머 공격을 당한 노드와 그렇지 않은 노드의 전송용량을 비교하였을 때 그 차이가 매우 적음을 알 수 있다. 즉, deception mechanism에서의 최대 최소값의 차이는 제안된 기법에서의 최대 최소값의 차이보다 5배 이상 차이가 나는 것을 알 수 있다. 그러므로 제안된 기법이 deception mechanism보다 전체 달성가능한 네트워크 전송용량이 다소 적을 수는 있으나 형평성 측면에서 매우 우수한 성능을 보임을 알 수 있다.

네트워크에서 사용 가능한 전체 채널의 개수 L이 변화하였을 때 채널도약 기법의 성능에 어떠한 영향

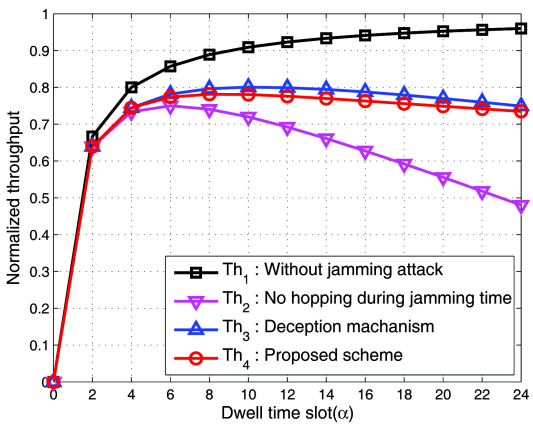


그림 4. DT 슬롯($\alpha$) 변화에 따른 규준화된 네트워크 데이터 전송용량
Fig. 4. Normalized network data throughput with varying dwell time slot($\alpha$)

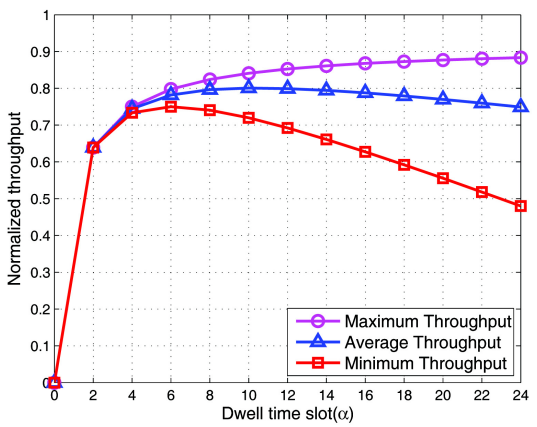


그림 5. Deception mechanism의 형평성 성능 결과
Fig. 5. Fairness performance result of the deception mechanism

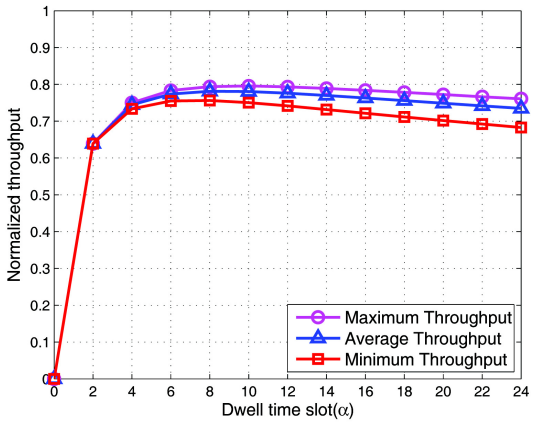


그림 6. 제안된 채널도약 기법의 형평성 성능 결과
Fig. 6. Fairness performance result of the proposed scheme

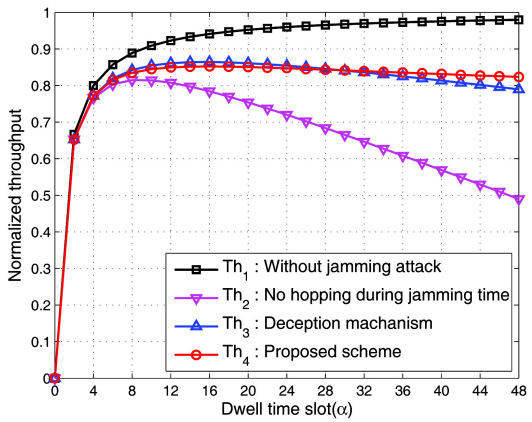


그림 7. 전체채널의 수가 24 일때의 DT 슬롯($\alpha$) 변화에 따른 규준화된 네트워크 데이터 전송용량
Fig. 7. Normalized network data throughput with varying dwell time slot($\alpha$) when the total number of channel is 24

을 미치는지 살펴보기 위하여 L을 12에서 24로 변화시켰을 경우 제안된 채널도약 기법과 deception mechanism의 전송용량에 관한 성능을 그림 7에 나타내었다. 전체 가용 채널의 수가 증가하였으므로 스마트 재머가 모든 채널을 한번씩 스캔할 수 있는 시간을 고려하여 DT 구간 슬롯($\alpha$)을 48까지 고려하였다. 형평성에 관한 결과는 전체 가용 채널의 개수와 무관하게 재밍당하는 노드의 희생을 강요하는 deception mechanism 보다 제안된 기법의 성능이 훨씬 우수하며 그림 5, 6의 결과와 유사하므로 생략하였으나 달성가능한 네트워크 전송용량은 그림 7에서 보는바와 같이 DT 슬롯 $\alpha$값이 28보다 큰 구간에서 오히려 deception mechanism 보다 제안된 기법의 전송용량이 다소 크다는 것을 알 수 있다. 즉, 네트워크내에 사용자 노드의 수가 많지 않고 DT 구간이 긴 상황에서는 재머를 유인하기 위해 하나의 노드가 희생하여 나머지 노드들의 전송용량을 보장해주는 기법은 형평성뿐만 아니라 달성가능한 전송용량의 측면에서도 효과가 떨어지므로 본 논문에서 제안된 기법을 적용하는 것이 효과적임을 알 수 있다.

## V. 결 론

본 논문에서는 802.11 전술 무선랜 환경에서 채널을 스캔하여 사용중인 채널을 찾아낸 후 재밍을 실시하는 스마트 재머 공격시 피해를 최소화 할 수 있는 채널도약 기법에 관하여 살펴보았다. 특히, 재밍 공격시 네트워크의 달성가능한 규준화된 네트워크 데이터 전송용량을 계산할 수 있는 분석모델을 제시하여 기존에 제안된 deception mechanism의 장단점을 분석하였으며 이를 바탕으로 군 전술통신 환경에 더욱 적합한 채널도약 기법으로 특정 사용자 노드에게 재밍이 집중되는 현상을 방지하여 노드들 간의 형평성 문제를 해결할 수 있는 새로운 채널도약 기법을 제안하였다. 분석 모델을 이용하여 제안된 기법의 성능이 기존의 deception mechanism 보다 달성가능한 데이터 전송용량은 다소 감소할 수 있으나 사용자 노드들 간의 형평성은 매우 큰 폭으로 향상 시킬 수 있음을 보여주었다.

## References

[1] S. Shanken, D. Hughes, and T. Carter, "Secure wireless local area network (SWLAN)," in *Proc. IEEE MILCOM*, vol. 2, pp. 886-891, Nov. 2004.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. MobiHoc'05*, pp. 46-57, Urbana-Champaign, IL, USA, May 2005.

[3] N. Sufyan, N. A. Saqib, and Z. Muhammad, "Detection of jamming attacks in 802.11b wireless networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 208, 2013.

[4] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks,"

in *Proc. INFOCOM '07*, pp. 2526-2530, Anchorage, AK, May 2007.

[5] S. Jeong, J. Jeung, and J. Lim, "Measurement-based channel hopping scheme against jamming attacks in IEEE 802.11 wireless networks," *J. KICS*, vol. 37, no. 4, pp. 205-213, Apr. 2012.

[6] E.-K. Lee, S.-Y. Oh, and M. Gerla, "Randomized channel hopping scheme for anti-jamming communication," *IEEE 2010 IFIP, Wireless Days (WD)*, pp. 1-5, Venice, Italy, Oct. 2010.

[7] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *Proc. IEEE SIGCOMM*, vol. 37, pp. 385-396, Aug. 2007.

[8] M. S. Gast, *802.11 wireless networks: the definitive guide*, O'Reilly publisher, 2002.

[9] S. Khattab, D. Mosse, and R. Melhem, "Jamming mitigation in multi-radio wireless networks: reactive or proactive?," in *Proc. SecureComm*, no. 27, pp. 1-10, Sept. 2008.

[10] J. Jeung, S. Jeong, and J. Lim, "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN," in *Proc. IEEE MILCOM*, pp. 1231-1236, Baltimore, MD, Nov. 2011.

**김 용 철** (Yongchul Kim)

1998년 3월 : 육군사관학교 전자공학과 학사

2001년 11월 : University of Surrey, UK 전자공학과 석사

2011년 12월 : North Carolina State University, USA 전기컴퓨터 공학과 박사

2012년 2월~현재 : 육군사관학교 전자공학과 부교수

<관심분야> WiMAX, Relay Networks, Ad-hoc Networks, Wireless Jamming.