논문 18-43-04-01 The Journal of Korean Institute of Communications and Information Sciences '18-04 Vol.43 No.04
https://doi.org/10.7840/kics.2018.43.4.619

# 물리계층 보안을 위한 이종 망에서 소형 기지국의 역할: 전파방해 혹은 협력

방 인 규◆, 김 수 민°

# A Role of Small Cells in Heterogeneous Networks for Physical-Layer Security: Jamming or Cooperation

Inkyu Bang◆, Su Min Kim°

요 약

본 논문에서는 이종망에서 물리계층 보안을 위한 소형 기지국의 역할을 분석한다. 소형 기지국이 채널 상황에 따라 도청자의 신호 수신 능력을 저하시킬 수 있는 전파방해 혹은 사용자의 신호 품질을 향상시킬 수 있는 협력전송을 수행한다는 전제 하에 다음의 사항을 분석한다. 첫째, 사용자의 수, 도청자의 수, 사용자 선택 방식이 소형 기지국의 전파방해 전략(전파방해 혹은 협력전송)에 미치는 영향을 수학적으로 분석한다. 둘째, 모의실험을 통해 제안하는 사용자 선택 방식과 전파방해 전략의 타당성을 보안 전송률 관점에서 확인한다. 그 결과, 소형 기지국은 도청자의 채널 정보 이용가능 여부에 따라 두 가지 전파방해 전략을 사용할 수 있음을 확인하였다. 소형 기지국이 도청자의 정확한 채널 정보를 알 수 있는 경우, 소형 기지국은 적응적 전파방해 전략을 사용한다. 소형 기지국은 사용자와 도청자의 순시 채널을 확인하여 매순간 전파방해 혹은 협력전송의 수행 여부를 정확히 선택한다. 소형 기지국이 도청자의 통계적 채널 정보만을 이용할 수 있는 경우, 소형 기지국은 확률적 전파방해 전략을 사용한다. 이 경우, 도청자의 순시 채널을 모르기 때문에 매순간 특정 확률로 전파방해 혹은 협력전송의 수행 여부를 선택한다.

**키워드** : 물리계층 보안, 기회주의적 전파방해, 사용자 스케줄링, 이종망, 보안 전송률

**Key Words** : Physical Layer Security, Opportunistic Jamming, User Scheduling, Heterogeneous Networks, Secrecy Rate

ABSTRACT

In this paper, we investigated a role of small cell in heterogeneous networks for physical layer security. We assume that the small cell can be used for jamming to degrade an eavesdropper's capability or for cooperative transmission to enhance a user's signal quality. When we consider multiple users and eavesdroppers, we analyzed the effect of the number of users, eavesdroppers, and user selection on jamming strategies. We also verified the effectiveness of the proposed user selection and jamming strategies in terms of secrecy rate through simulations. Finally, we proposed jamming strategies at the small cell depending on the availability of the eavesdropper's channel state information (CSI). The small cell adopts an adaptive jamming if the eavesdropper's CSI is available otherwise it utilizes probabilistic jamming.

※ 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016R1C1B1014069).
◆ First Author : (ORCID:0000-0001-7109-1999)Department of Computer Science, National University of Singapore, inkyu@comp.nus.edu.sg, 정회원
° Corresponding Author : (ORCID:0000-0002-5951-9208)Department of Electronics Engineering, Korea Polytechnic University, suminkim@kpu.ac.kr, 정회원
논문번호 : KICS2017-12-403, Received December 26, 2017; Revised March 16, 2018; Accepted March 16, 2018

## Ⅰ. 서 론

오늘날 무선통신은 사용의 편리함과 유용성으로 인해 우리의 일상생활에서 널리 사용되고 있다. 그러나 무선통신 시스템은 사용자 정보가 무선채널을 통해 노출될 수 있다는 근본적인 취약점을 지니고 있다. 따라서 도청자(혹은 악의적 사용자)는 무선 신호의 전파 특성을 이용하여 사용자의 정보를 손쉽게 도청할 수 있다. 일상생활에 무선 기기의 사용이 급증하고 있는 추세를 비추어 볼 때, 무선 보안(wireless security) 문제는 앞으로 더욱 중요해질 것으로 예상된다. 이러한 흐름에 맞춰 최근 무선통신분야에서는 무선 채널에서 정보이론 관점의 기밀성을 보장하는 물리계층 보안(physical layer security)이 새로운 연구 분야로 주목을 받고 있다.

Shannon과 Wyner의 연구를 기점으로[1,2], 물리계층 보안에 대한 본격적인 연구들이 시작되었다. 전통적으로 물리계층 보안 연구에서는 송신기, 수신기, 도청자로 구성된 네트워크를 기본 시스템 모델로 삼는다[3,4]. 최근 많은 연구가 다중 사용자 네트워크 환경에서 물리계층 보안 문제에 집중하기 시작하였다[5-8]. 2014년도 조사 논문에서는 다중 사용자 네트워크 환경에서 물리계층 보안에 대한 전반적인 연구흐름을 분석하였다[5]. 이후에도 수신기에 다중 안테나 혹은 분산 안테나가 장착되었을 때 최적 보안 전송률 달성을 위한 다중 사용자 스케일링 법칙에 관한 연구[6,7], 송신 전력조절이 보안 전송률에 미치는 영향 분석에 관한 연구[8] 등이 이루어졌다.

다른 한편으로 도청자의 무선 신호 도청을 효과적으로 방해하기 위해 조력자(a helper) 및 인공 잡음(artificial noise)의 개념을 도입한 연구들이 있다[9-14]. Goel의 논문은 다중 안테나 혹은 중계기 등을 통해 만들어진 인공 잡음이 최소한의 보안 용량(secrecy capacity)을 보장하는데 효과적임을 보였다[9]. 추가로 McKay의 논문에서는 인공 잡음의 효과를 극대화하기 위한 데이터와 인공 잡음 사이의 최적 전력 할당 방식이 제안되었다[10]. Ding의 논문은 중계 네트워크에서 상황에 따른 기회주의적 중계 방법이 사용자의 보안 성능을 향상시킬 수 있음을 보였으며[11], Lee의 논문에서도 보안 성능을 향상시키기 위한 기회주의적 전파방해기 선택 방법이 제안되었다[12]. Bang의 논문에서는 단일 도청자가 존재하는 상황에서 소형 기지국 혹은 데이터 전송을 하지 않는 사용자를 활용하여 인공 잡음을 생성하는 기법이 제안되었다[13,14].

본 논문에서는 이종 망에서 물리계층 보안을 위한 소형 기지국의 역할을 분석한다. 본 논문은 소형 기지국이 채널 상황에 따라 도청자의 신호 수신 능력을 저하시킬 수 있는 전파방해 혹은 사용자의 신호 품질을 향상시킬 수 있는 협력전송을 수행한다는 전제 하에 다음의 사항을 분석한다. 첫째, 다중 사용자 및 다수의 도청자를 고려하여, 사용자의 수, 도청자의 수, 사용자 선택 방식이 소형 기지국의 전파방해 전략에 미치는 영향을 수학적으로 분석한다. 둘째, 모의실험을 통해 제안하는 사용자 선택 방식과 전파방해 전략의 타당성을 보안 전송률 관점에서 확인한다.

본 논문은 총 6장으로 구성되어있으며. 각 장의 내용은 다음과 같다. Ⅱ장에서는 본 논문에서 전제하는 시스템 모델 및 변수들을 설명한다. Ⅲ장에서는 이종 망에서 소형 기지국의 동작에 따른 보안 전송률 최적화 문제를 소개한다. Ⅳ장에서는 보안 전송률을 증가시킬 수 있는 사용자 선택 방법과 전파방해 전략을 제안한다. Ⅴ장에서는 제안 기법(사용자 선택 및 전파방해 전략)에 대한 모의실험 기반의 성능평가 결과를 소개한다. 마지막으로 Ⅵ장에서는 본 논문에서 논의된 내용을 다시 한 번 상기하며 최종 결론을 짓는다.

## Ⅱ. 시스템 모델

### 2.1 시스템 환경 및 변수

본 논문에서는 하나의 기지국(macro base station) 및 이를 지원하는 하나의 소형기지국(small base station) 그리고 $N$명의 사용자와 $K$명의 도청자가 존재하는 하향링크(downlink) 이종 망을 고려한다. 모든 구성 요소들은 하나의 안테나를 지닌다고 가정하였으며 기지국과 소형 기지국은 유선을 통해 서로의 정보(예, 채널 정보)를 교환할 수 있다고 가정하였다. 또한, 한 심벌 슬롯동안 오직 하나의 사용자만이 선택되어 기지국과 소형기지국으로부터 하향링크 서비스를 받는다. 도청자들은 서로 협력 없이 독립적으로 사용자의 무선 신호에 담긴 정보를 엿듣는다. 그림 1은 $N=3$, $K=2$일 때 시스템 모델 예시를 나타낸다.

기지국은 선택된 사용자를 위해 항상 데이터를 전송하며 소형기지국은 상황에 따라 전파방해 혹은 기지국과의 협력전송을 수행한다. 본 논문에서는 이와 같은 소형기지국의 운영방식을 기회주의적 전파방해(opportunistic jamming)라고 표현하고 소형기지국의 동작모드를 이진 값을 갖는 변수 $r\in\{0,1\}$로 정의하였다. $r=1$인 경우, 소형기지국은 전파방해를 위해 동작하고 $r=0$인 경우, 소형기지국은 기지국과의 협력통신을 수행한다.

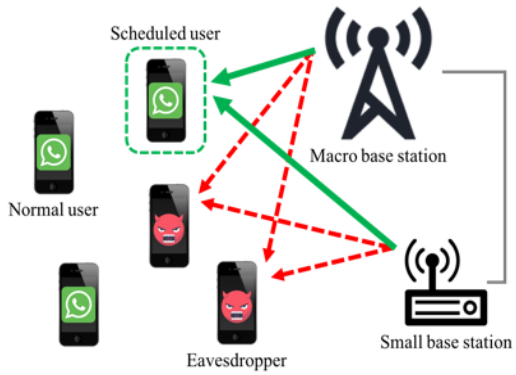


그림 1. 시스템 모델: $N=3$, $K=2$ 예시.
Fig. 1. System model: an example of $N=3$, $K=2$.

$P_m$, $P_s$, $\sigma_0^2$은 각각 기지국, 소형기지국에서 송신 전력과 사용자의 수신 잡음 전력의 크기를 나타낸다. 분석의 편의상 $n$번째 사용자가 선택된 사용자라고 가정하며($n \in \{1,\cdots,N\}$), 이때 사용자와 기지국 혹은 소형기지국 사이의 채널은 $h_{m,n}$, $h_{s,n}$으로 표현한다. 유사하게 $k$번째 도청자($k \in \{1,\cdots,K\}$)와 기지국 혹은 소형기지국 사이의 채널은 $g_{m,k}$, $g_{s,k}$으로 표현한다. 각 채널 계수는 독립 가우시안 분포를 따르는 레일리(Rayleigh) 채널 모델을 따른다, 즉, $h_{m,n} \sim CN(0,\sigma_{m,n}^2)$ 과 $g_{m,k} \sim CN(0,\sigma_{m,k}^2)$이 되며, $h_{s,n} \sim CN(0,\sigma_{s,n}^2)$ 그리고 $g_{s,k} \sim CN(0,\sigma_{s,k}^2)$이 된다. 여기서 채널의 분산 값은 두 통신 노드사이의 경로감쇄 효과를 근사적으로 포함할 수 있다[15]. 기지국과 소형기지국은 사용자의 피드백을 통해 사용자의 채널 상태 정보(channel state information or CSI)를 알 수 있다($h_{m,n}$, $h_{s,n}$). 본 논문에서는 도청자의 채널 상태 정보의 이용가능 여부에 따라 도청자에 대한 다음의 두 가지 채널 가정을 사용한다.

- 강한 채널 가정: 기지국과 소형기지국은 도청자의 순간적인 채널 상태 정보를 정확히 알 수 있다[16].
- 약한 채널 가정: 기지국과 소형기지국은 도청자의 순간적인 채널 상태 정보는 알 수 없으며, 통계적인 채널 정보만을 알 수 있다(평균 채널 품질, 즉, $\sigma_{m,k}^2$, $\sigma_{s,k}^2$)[17].

### 2.2 사용자 및 도청자의 수신 신호 표현

보안 전송률 분석을 위해서는 사용자 및 도청자의 수신 신호 및 수신 신호 대 잡음비(signal to noise ratio or SNR) 분석이 필요하다. 소형기지국의 동작모드 $r$의 값에 따라 사용자와 도청자의 수신 신호 및 수신 SNR은 다르게 표현된다. 사용자의 정보와 인공잡음 전송에는 위상 편이 변조(Phase Shift Keying) 방식을 사용한다고 가정한다. 또한 기지국과 소형기지국이 협력전송을 할 경우 두 신호간의 동기화 문제는 충분히 해결가능하다고 가정하였다[15].

#### 2.2.1 전파방해($r=1$)

기지국은 사용자 정보 $u$을 전송하고 소형지기국은 인공잡음 $x$을 전송한다. 이때 사용자의 수신 신호와 수신 SNR은 각각 다음과 같다.

$$y_n(r=1) = h_{m,n}\sqrt{P_m}u + h_{s,n}\sqrt{P_s}x + w_n, \quad (1\text{-}1)$$

$$\gamma_n(r=1) = \frac{|h_{m,n}|^2 P_m}{|h_{s,n}|^2 P_s + \sigma_0^2}, \quad (1\text{-}2)$$

여기서 $w_n$은 사용자의 수신 백색잡음을 나타낸다. 유사하게 $k$번째 도청자의 수신 신호와 수신 SNR은 각각 다음과 같다.

$$y_k(r=1) = g_{m,k}\sqrt{P_m}u + g_{s,k}\sqrt{P_s}x + w_k, \quad (2\text{-}1)$$

$$\gamma_k(r=1) = \frac{|g_{m,k}|^2 P_m}{|g_{s,k}|^2 P_s + \sigma_0^2}, \quad (2\text{-}2)$$

여기서 $w_k$은 $k$번째 도청자의 수신 백색잡음을 나타낸다.

#### 2.2.2 협력통신($r=0$)

기지국과 소형기지국은 협력통신을 이용하여 사용자 정보 $u$를 전송한다. 협력통신은 도청자의 채널 가정 여부와 상관없이 기지국과 소형기지국의 채널 상황만을 이용할 수 있는 정합 필터(matched filter) 기반의 송신 빔형성 기법을 사용한다[18]. 따라서 기지국과 소형기지국은 사용자 정보 $u$에 채널 정보 기반의 가중치를 $\alpha_n = h_{m,n}^*/|h_{m,n}|$과 $\beta_n = h_{s,n}^*/|h_{s,n}|$을 곱한 신호를 각각 전송한다. 이때 사용자의 수신 신호와 수신 SNR은 각각 다음과 같다.

$$y_n(r=0) = h_{m,n}\sqrt{P_m}\alpha_n u + h_{s,n}\sqrt{P_s}\beta_n u + w_n, \quad (3\text{-}1)$$

$$\gamma_n(r=0) = \frac{(|h_{m,n}|\sqrt{P_m} + |h_{s,n}|\sqrt{P_s})^2}{\sigma_0^2}, \quad (3\text{-}2)$$

여기서 기지국과 소형기지국은 협력통신을 수행했기 때문에 수식 (1-2)의 결과와는 다르게 수신 SNR에 인공잡음으로 인한 간섭 효과가 발생하지 않는다. 마찬가지 방식으로 $k$번째 도청자의 수신 신호와 수신 SNR은 각각 다음과 같다.

$$y_k(r=0)=g_{m,k}\sqrt{P_m}\alpha_n u+g_{s,k}\sqrt{P_s}\beta_n u+w_k, \tag{4-1}$$

$$\gamma_k(r=0)=\left|\frac{g_{m,k}h_{m,n}^*}{|h_{m,n}|}P_m+\frac{g_{s,k}h_{s,n}^*}{|h_{s,n}|}P_s\right|^2/\sigma_0^2, \tag{4-2}$$

여기서 빔형성 가중치 $\alpha_n$과 $\beta_n$은 사용자를 기준으로 설정되었기 때문에 도청자의 수신 SNR은 사용자의 수신 SNR보다 복잡하게 표현된다. 따라서 보안 전송률 분석할 때 이러한 부분을 잘 고려해야 한다.

## Ⅲ. 보안 전송률 최적화 문제

기본적으로 보안 전송률은 사용자의 전송률과 도청자의 전송률 차이로 정의할 수 있다. 단, 본 논문에서는 $K$개의 독립적인 도청을 전제하기 때문에 $K$개의 도청 시도 중에 가장 효과적인 도청시도만이 보안 전송률에 반영된다. 따라서 보안 전송률은 소형기지국의 동작모드 $r$의 함수로 다음과 같다.

$$C_n(r)=\left[\log(1+\gamma_n(r))-\log(1+\max_k\{\gamma_k(r)\})\right]^+, \tag{5}$$

여기서 $[x]^+=\max\{x,0\}$을 나타내며 $\gamma_n(r)$과 $\gamma_k(r)$은 $r$의 값에 따라 수식 (1) ~ (4)을 이용하여 계산할 수 있다. 결국 기회주의적 전파방해를 사용했을 때 보안 전송률은 다음과 같다.

$$C(n,r)=r\times C_n(1)+(1-r)\times C_n(0). \tag{6}$$

수식 (6)의 보안 전송률은 사용자 선택 ($n$의 선택)과 전파방해 전략($r$값 설정)에 따라 달라질 수 있다. 따라서 보안 전송률 최적화 문제를 다음과 같이 설정할 수 있다.

$$(n^\star,r^\star)=\arg\max_{(n,r)}\{C(n,r)\}. \tag{7}$$

수식 (7)의 최적 해를 분석적으로 찾는 것은 쉽지 않다. 단, 수식 (7)의 최적 해의 보안 성능은 무차별검색(exhaustive search) 방식을 통해 검증할 수 있다. 실제로 최적 해를 이용했을 때의 보안 성능은 최고로 우수할 것이지만 본 논문에서는 수학적 분석이 가능한 최적화 문제를 다루고자 한다. 따라서 본 논문에서는 수식 (7)의 최적화 문제 대신 $C(n,r)$의 하한(lower bound)을 고려하여 새로운 최적화 문제에 설정하였으며 이는 다음과 같다.

$$(n^\dagger,r^\dagger)=\arg\max_{(n,r)}\{\overline{C}(n,r)\}, \tag{8}$$

여기서 $\overline{C}(n,r)$은 $C(n,r)$의 하한으로 모든 $n$과 $r$에 대하여 $C(n,r)\geq\overline{C}(n,r)$을 만족한다. $\overline{C}(n,r)$을 구하기 위해서 우선 몇 가지 변수를 다음과 같이 정의한다.

$$\mu_h(n)=|h_{m,n}|^2P_m+|h_{s,n}|^2P_s+\sigma_0^2,, \tag{9-1}$$

$$\lambda_h(n)=|h_{m,n}||h_{s,n}|\sqrt{P_mP_s}, \tag{9-2}$$

$$\theta_h(n)=|h_{s,n}|^2P_s+\sigma_0^2, \tag{9-3}$$

$$\mu_g(k)=|g_{m,k}|^2P_m+|g_{s,k}|^2P_s+\sigma_0^2, \tag{9-4}$$

$$\lambda_g(k)=|g_{m,k}||g_{s,k}|\sqrt{P_mP_s}, \tag{9-5}$$

$$\theta_g(k)=|g_{s,k}|^2P_s+\sigma_0^2, \tag{9-6}$$

여기서 $\lambda_h(n)$과 $\lambda_g(k)$은 항상 0이상의 값을 지닌다는 것을 알 수 있다. 수식 (9)을 이용하면 사용자 및 도청자의 수신 SNR 관련된 다음의 부등식들을 얻을 수 있다.

$$1+\gamma_n(1)=\frac{\mu_h(n)}{\theta_h(n)}, \tag{10-1}$$

$$1+\gamma_k(1)\leq\frac{\mu_g(k)+\lambda_g(k)}{\theta_g(k)}=1+\hat{\gamma}_k(1), \tag{10-2}$$

$$1+\gamma_n(0)\geq\frac{\mu_h(n)}{\sigma_0^2}=1+\bar{\gamma}_n(0), \tag{10-3}$$

$$1+\gamma_k(0)\leq\frac{\mu_g(k)+\lambda_g(k)}{\sigma_0^2}=1+\hat{\gamma}_k(0). \tag{10-4}$$

즉, $\hat{\gamma}_k(1)=\dfrac{|g_{m,k}|^2P_s+|g_{m,k}||g_{s,k}|\sqrt{P_mP_s}}{|g_{s,k}|^2P_s+\sigma_0^2}$ 그리고 $\overline{\gamma}_n(0)=\dfrac{|h_{m,n}|^2P_m+|h_{s,n}|^2P_s}{\sigma_0^2}$ 으로 정의할 수 있으며 각각은 도청자 $k$와 사용자 $n$의 수신 SNR 상한(upper bound) 및 하한(lower bound)을 나타낸다.

수식 (10)을 이용하면 소형기지국의 동작모드 값에 따른 수식 (5)의 하한을 다음과 같이 구할 수 있다.

$$\overline{C}_n(1)=\left[\log\left(\frac{1+\gamma_n(1)}{1+\max_k\{\hat{\gamma}_k(1)\}}\right)\right]^+\le C_n(1), \tag{11-1}$$

$$\overline{C}_n(0)=\left[\log\left(\frac{1+\overline{\gamma}_n(0)}{1+\max_k\{\hat{\gamma}_k(0)\}}\right)\right]^+\le C_n(0). \tag{11-2}$$

따라서 $C(n,r)\ge\overline{C}(n,r)$을 만족하는 $\overline{C}(n,r)$은 다음과 같이 정의할 수 있다.

$$\overline{C}(n,r)=r\times\overline{C}_n(1)+(1-r)\times\overline{C}_n(0). \tag{12}$$

$\overline{C}(n,r)$은 $C(n,r)$의 하한이므로 $\overline{C}(n,r)$을 이용하는 수식 (8)의 최적화 문제를 풀고 이러한 사용자 선택 방식과 전파방해 전략을 사용할 경우 $(n^\dagger,r^\dagger)$, 실제로는 이 보다 높은 보안 전송률을 달성할 수 있다.

## Ⅳ. 사용자 선택과 전파방해 전략

본 장에서는 보안 전송률을 증가시키기 위한 2가지 사용자 선택 방법을 제시한다. 또한 도청자의 채널 정보 이용가능 여부에 따른 전파방해 전략을 제안한다. 소형기지국은 강한 채널 가정에서는 적응적 전파방해(adaptive jamming)를 수행하고 약한 채널 가정에서는 확률적 전파방해(probabilistic jamming)를 수행한다.

수식 (9)을 이용하여 수식 (12)을 다음과 변형시킬 수 있다.

$$\overline{C}(n,r)=\left[\log\left(\frac{\mu_h(n)}{\mu_g(k^*)+\lambda_g(k^*)}\times\left(\frac{\theta_g(k^*)}{\theta_h(n)}\right)^r\right)\right]^+, \tag{13}$$

여기서 $k^*=\arg\max_k\{\overline{\gamma}_k(r)\}$을 나타낸다.

### 4.1 사용자 선택 기준

수식 (13)의 로그 함수는 단조 증가함수이다. 본 장에서는 로그 함수안의 변수인 $\dfrac{\mu_h(n)}{\mu_g(k^*)+\lambda_g(k^*)}$을 극대화시키는 사용자 $n$을 선택한 이후에 $\theta_h(n)$과 $\theta_g(k^*)$ 값의 비율에 따라 소형기지국의 동작모드 값을 결정하는 사용자 선택 및 전파방해 전략을 소개한다. 먼저 $\mu_h(n)$을 극대화시키기 위한 사용자 선택 방법으로 두 가지 사용자 선택 방식을 제안한다.

#### 4.1.1 가중 합 사용자 선택(Weight-sum user selection or WUS)

$\mu_h(n)$은 $|h_{m,n}|^2P_m+|h_{s,n}|^2P_s+\sigma_0^2$이기 때문에 사용자와 기지국 및 소형기지국 사이의 채널의 가중 합 $|h_{m,n}|^2P_m+|h_{s,n}|^2P_s$을 고려할 경우 $\mu_h(n)$을 극대화할 수 있다. 따라서 WUS를 사용할 경우 선택되는 사용자는 다음과 같다.

$$n^*_{WUS}=\arg\max_n\{|h_{m,n}|^2P_m+|h_{s,n}|^2P_s\}. \tag{14}$$

#### 4.1.2 순차적 사용자 선택(Sequential user selection or SUS)

순차적 사용자 선택기준은 분석의 용이함을 위해 기지국과 사용자 사이의 채널 및 소형기지국과 사용자 사이의 채널 값을 순차적으로 비교하여 사용자를 선택하는 기준이다. 순차적 사용자 선택 기준을 사용할 경우 전파방해에 관한 수학적 분석이 용이해지며 이는 도청자의 통계적 채널 정보만을 활용하여 확률적으로 전파방해 전략 수립에 도움이 된다. SUS를 사용할 경우 선택되는 사용자는 다음과 같다.

$$n_1^*=\arg\max_n\{|h_{m,n}|^2\}, \tag{15-1}$$

$$n_2^*=\arg\max_n\{|h_{s,n}|^2\}, \tag{15-2}$$

$$n^*_{SUS}=\begin{cases}n_1^* & \text{if } |h_{m,n_1^*}|^2\ge|h_{s,n_1^*}|^2\\ n_2^* & \text{if } |h_{m,n_2^*}|^2<|h_{s,n_2^*}|^2\end{cases}. \tag{15-3}$$

### 4.2 적응적 전파방해 전략(Adaptive Jamming Strategy: AJS)

강한 채널 가정에서 소형기지국은 모든 도청자의 순시 채널 정보($g_{m,k}$, $g_{s,k}$)를 알 수 있다. 이 경우 소

형기지국은 사용자 선택 기준에 따라 선택된 사용($n^*_{WUS}$ 혹은 $n^*_{SUS}$)를 기준으로 $\theta_h(n)$을 계산한 이후에 주어진 도청자의 채널 정보를 활용하여 $\theta_g(k^*)$값을 계산할 수 있다. $\theta_g(k^*) \geq \theta_h(n)$인 경우 $r=1$로 설정하고 반대의 경우 $r=0$으로 설정하여 주어진 사용자 선택 방식에서 수식 (13)을 극대화할 수 있다. 따라서 적응적 전파방해 전략의 $r$값 설정은 다음과 같다.

$$r^*_{AJS}=\begin{cases}1 & \text{if}\,|h_{s,n}|^2 \leq \max_k\{|g_{s,k}|^2\} \\ 0 & \text{if}\,|h_{s,n}|^2 > \max_k\{|g_{s,k}|^2\}\end{cases}. \tag{16}$$

### 4.3 확률적 전파방해 전략(Probabilistic Jamming Strategy: PJS)

약한 채널 가정에서 소형기지국은 도청자의 순시 채널 정보를 알 수 없기 때문에 AJS와 같은 정교한 전파방해 전략을 사용할 수 없다. 하지만 채널의 통계적 특성(채널 분포, 평균 및 분산)을 이용하면 수식 (16)의 $|h_{s,n}|^2$와 $\max_k\{|g_{s,k}|^2\}$의 대소 관계를 확률적으로 계산할 수 있다. 예를 들어 $r=1$에 해당하는 사건인 $|h_{s,n}|^2 \leq \max_k\{|g_{s,k}|^2\}$의 발생확률이 0.3이라면 이는 10개의 심벌 슬롯 동안 평균적으로 3개의 심벌 슬롯에서 전파방해 전략이 사용되고 나머지 7새의 심벌 슬롯에서는 협력전송이 사용되는 것을 의미한다. 따라서 본 논문에서는 이러한 확률기반의 전파방해를 확률적 전파방해 전략(PJS)이라고 정의하였다. 확률적 전파방해 전략의 $r$값 설정은 다음과 같다.

$$r^*_{PJS}=\begin{cases}1 & \text{with}\ \Pr\{|h_{s,n}|^2 \leq \max_k\{|g_{s,k}|^2\}\}=p^* \\ 0 & \text{with}\ 1-p^*\end{cases}. \tag{17}$$

PJS은 사용자 선택기준에 상관없이 모두 적용가능하다. 하지만 WUS 기준을 사용할 경우 분석적으로 확률 $p^*$을 계산하는 것이 어렵기 때문에 경험적 데이터들을 통한 수치적 확률을 계산해야 한다. 반면 SUS 기준을 사용할 경우 확률 $p^*$에 대한 수학적인 분석이 가능하다. 따라서 본 장의 나머지부분에서는 SUS 기준을 사용할 경우 PJS의 확률 $p^*$에 대한 분석에 집중한다.

수식 (15)의 사용자 인덱스($n^*_1$, $n^*_2$, $n^*_{SUS}$)를 이용하여 분석에 필요한 확률 변수를 다음과 같이 정의할 수 있다.

$$X_0=|h_{s,n^*_{SUS}}|^2, \tag{18-1}$$

$$X_1=|h_{m,n^*_1}|^2, \tag{18-2}$$

$$X_2=|h_{s,n^*_2}|^2, \tag{18-3}$$

$$Y=\max_k\{|g_{s,k}|^2\}, \tag{18-4}$$

여기서 네 확률 변수는 서로 독립이다. 수식 (18)을 이용하면 확률 사건 $|h_{s,n}|^2 \leq \max_k\{|g_{s,k}|^2\}$을 다음과 같이 표현할 수 있다.

$$\begin{aligned}p^* &= \Pr\{|h_{s,n^*_{SUS}}|^2 \leq \max_k\{|g_{s,k}|^2\}\} \\ &= \Pr\{X_0 \leq Y\} \\ &= \Pr\{X_0 \leq Y | X_1 > X_2\}\Pr\{X_1 > X_2\} \\ &\quad + \Pr\{X_0 \leq Y | X_1 \leq X_2\}\Pr\{X_1 \leq X_2\}.\end{aligned} \tag{19}$$

기본적으로 사용자 선택을 고려하지 않았을 때, $|h_{m,n}|^2$와 $|h_{s,n}|^2$, 은 각각 지수분포를 따르며 $|g_{s,k}|^2$은 도청자의 채널이기 때문에 사용자 선택 여부와 관계없이 항상 지수분포를 따른다. 따라서 $X_1$, $X_2$, $Y$은 각각 지수분포를 따르는 여러 확률 변수 중 최댓값을 선택했을 때의 확률 변수를 의미한다. 즉, $X_1$과 $X_2$은 $N$개의 지수 확률 변수를 고려했을 때의 최댓값이며 $Y$의 $K$개의 지수 확률 변수를 고려했을 때의 최댓값이 된다.

$\Pr\{X_1 \leq X_2\}$은 확률 변수들 간의 함수 관계를 이용하여 다음과 같이 계산할 수 있다[19].

$$\Pr\{X_1 \leq X_2\}=\int_0^\infty F_{X_1}(y)f_{X_2}(y)dy, \tag{20}$$

여기서 $F_{X_1}(x)$와 $f_{X_2}(x)$은 각각 $X_1$과 $X_2$의 누적분포함수와 확률밀도함수를 나타낸다. 순서 통계(order statistics)를 이용하면 $F_{X_1}(x)$와 $f_{X_2}(x)$을 어렵지 않게 계산할 수 있다. 더욱이 기지국과 사용자, 소형기지국과 사용자, 소형기지국과 도청자 사이의 평균 채널 품질을 나타내는 채널 분산 값을 모두 같다고 가정할 경우 $\Pr\{X_1 \leq X_2\}=0.5$이 된다(즉, $\sigma^2_{m,n}=\sigma^2_{s,n}=\sigma^2_{s,k}$). 또한 수식 (19)에서 $X_0$, $X_1$, $X_2$의 관계를 이용하면 $\Pr\{X_0 \leq Y | X_1 > X_2\}$의 $X_0$은 사용자 선택을 고려하지 않았을 때와 마찬가지로 지

수분포를 따르게 되어 $\Pr\{|h_{m,n}|^2 \le Y\}$ 으로 간략화 된다. 비슷하게 $\Pr\{X_0 \le Y | X_1 > X_2\}$은 $\Pr\{X_2 \le Y\}$으로 간략화 된다. 결국 $\Pr\{|h_n|^2 \le Y\}$ 와 $\Pr\{X_2 \le Y\}$은 확률 변수들 간의 함수관계와 적분공식을 활용하여 얻을 수 있다[19], [20].

최종적으로 SUS 기준을 사용하고 $\sigma_{m,n}^2 = \sigma_{s,n}^2 = \sigma_{s,k}^2$일 때, PJS의 $p^*$은 다음과 같다.

$$p^* = \frac{1}{2} \times \frac{K}{K+1} + \frac{1}{2} \times \frac{K}{K+2N}. \quad (21)$$

시스템에 존재하는 도청자의 수가 PJS의 전파방해 확률을 결정짓는 중요한 요소임을 수식 (21)을 통해서 확인할 수 있다. 또한 수식 (21)을 통해 사용자의 수가 무수히 많을 때 $p^*$ 값이 $\lim_{N\to\infty} p^* = \frac{K}{K+1}$ 으로 수렴하는 것을 확인할 수 있다. 비슷하게 도청자의 수가 무수히 많을 때는(사용자의 수는 고정) $p^*$ 값이 1로 수렴하는 것을 확인할 수 있다. 이는 도청자가 많아지면 어떤 심벌 슬롯에도 채널 값이 좋은 도청자가 존재할 확률이 증가하기 때문에 협력통신보다 전파방해가 보안 전송률을 높이는데 효과적임을 의미한다.

## V. 성능 평가

### 5.1 모의실험 환경

본 절에서는 모의실험을 위한 시스템 변수들의 설정 값을 소개한다. 모든 사용자들의 채널 품질과 모든 도청자들의 채널 품질은 균일하다고 가정하였다. 즉, $\sigma_{m,n}^2 = \sigma_1^2$, $\sigma_{s,n}^2 = \sigma_1^2$, $\sigma_{m,k}^2 = \sigma_3^2$, $\sigma_{s,k}^2 = \sigma_4^2$으로 설정하여 PJS의 분석 결과와 모의실험 결과를 비교하였다. 기지국과 소형기지국의 송신 전력은 송신 SNR값을 기준으로 10dB로 설정하였으며, 또한 정확성을 위하여 100,000번 이상의 반복 시행을 통해 모의실험의 결과를 얻었다.

모의실험을 통해 총 세 가지 제안 기법의 결과를 확인하였다: 첫 번째, 수식 (14)의 WUS 기준을 이용하여 사용자를 선택하고 AJS을 적용한 경우, 두 번째, 수식 (15)의 SUS 기준을 이용하여 사용자를 선택하고 AJS을 적용한 경우, 세 번째, 마찬가지로 SUS 기준을 사용하고 PJS을 적용한 경우. 성능 평가 및 비교를 위해서 제안 기법이외에도 모의실험에서는 다음의 세 가지 기법을 추가로 고려했다(각 비교 기법은 기지국과 사용자의 채널이 가장 좋은 사용자를 선택한다.):

- WCS (alWays Cooperation Scheme) - 소형기지국이 항상 협력통신을 위해 동작하는 기법
- RJS (Random Jamming Scheme) - 소형기지국이 항상 0.5의 확률로 전파방해 수행하는 기법
- WJS (alWays Jamming Scheme) - 소형 기지국이 항상 전파방해를 수행하는 기법

모의실험에서는 기지국과 사용자, 소형기지국과 사용자, 기지국과 도청자, 소형기지국과 도청자의 평균 채널 품질을 통해 이종 망 환경의 특성을 반영하였으며 설정 값에 따라 다음의 두 가지 시나리오를 고려하였다.

- 대칭 시나리오(Symmetric scenario): $\sigma_1^2 = 0$dB, $\sigma_2^2 = 0$dB, $\sigma_3^2 = 0$dB, $\sigma_4^2 = 0$dB.
- 비대칭 시나리오(Asymmetric scenario): $\sigma_1^2 = -3$ dB, $\sigma_2^2 = 0$dB, $\sigma_3^2 = -3$dB, $\sigma_4^2 = 0$dB.

대칭 시나리오는 기지국과 사용자, 소형기지국과 사용자, 기지국과 도청자, 소형기지국과 도청자 사이의 거리가 모두 비슷한 상황을 반영한다(모든 평균 채널 품질 값이 같음). 반면 비대칭 시나리오는 소형기지국과 사용자, 소형기지국과 도청자 사이의 거리가 기지국과 사용자, 기지국과 도청자 사이의 거리보다 상대적으로 더 가까운 상황을 반영한다. 일반적으로 소형기지국은 사용자와 가까운 위치에 설치되고 도청자 역시 소형기지국과 가까워질 확률이 높다. 따라서 이종 망 환경에서는 비대칭 시나리오가 조금 더 일반적인 상황이라고 할 수 있다.

### 5.2 수치적 결과

그림 2는 PJS의 분석 결과와 모의실험 결과를 비교하기 위해 $\sigma_1^2 = \sigma_2^2 = \sigma_4^2$을 가정하고 사용자 수와 도청자 수를 변화시켰을 때 전파방해 확률을 나타내는 그림이다. 수식 (21)의 결과를 활용하기 위해 사용자 선택 기준은 수식 (15)의 SUS 기준을 사용하였다. 기본적으로 본 논문에서 분석한 결과 값과 모의실험을 통해 얻은 값이 일치하는 것을 확인할 수 있다. 또한 수식 (21)의 유도과정에서 논의되었던 것처럼 도청자의 수가 증가할수록 전파방해 확률이 증가하는 것을 확인할 수 있다. 사용자의 수가 많은 경우에는 사용자 선택을 통해 다중사용자 다양화(multiuser

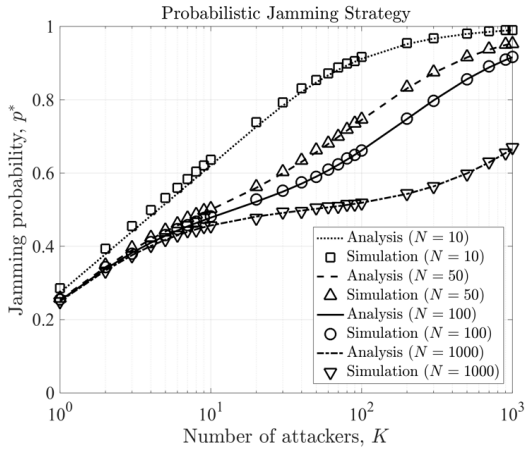


그림 2. SUS 기준을 적용했을 때 PJS의 전파방해 확률.
Fig. 2. Jamming probability of PJS with SUS.

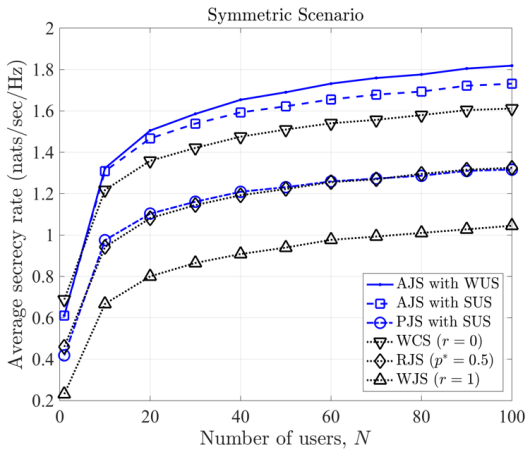


그림 3. 대칭 시나리오에서 사용자 수에 따른 보안 전송률.
Fig. 3. Average secrecy rate vs. $N$ (symmetric case).

diversity or MUD) 이득을 얻을 수 있기 때문에, 도청자의 수가 증가하더라도, 사용자의 수가 적은 경우보다 전파방해 확률이 천천히 증가하는 것을 확인할 수 있다. 결국, 도청자의 수 대비 사용자의 수 증가가 뚜렷할 경우 소형기지국은 협력 전송을 수행하는 것이, 반대로 사용자의 수 대비 도청자의 수의 증가가 뚜렷할 경우 소형기지국은 전파방해를 수행하는 것이 물리계층 보안 측면에서 효과적임을 확인할 수 있다.

그림 3은 대칭 시나리오에서 사용자의 수를 변화시켜가며 평균 보안 전송률을 관찰한 결과이며, 총 두 명의 도청자($K = 2$)가 존재한다고 가정하였다. 다중 사용자 다양화(MUD) 이득으로 인해서 사용자의 수가 증가할수록 제안 기법을 포함한 모든 기법의 평균 보안 전송률이 증가하는 것을 확인할 수 있다. 본 논문에서 AJS을 사용할 경우 사용자 선택 기준에 상관없이(WUS 혹은 SUS) 다른 기법들 보다 좋은 성능을 내는 것을 확인할 수 있다. 이는 AJS가 매 순간 도청자의 채널 정보를 정확히 활용하여 전파방해 혹은 협력 통신을 선택하기 때문이다. 반면, SUS 기준을 이용한 사용자 선택과 PJS를 결합할 경우 도청자의 통계적 채널 정보만을 활용하여 확률적 전파방해를 수행하기 때문에 AJS를 사용한 경우보다 성능이 좋지 않은 것을 확인할 수 있다. 또한 대칭 시나리오는 기지국과 사용자, 소형기지국과 사용자, 기지국과 도청자, 소형기지국과 도청자 사이의 거리가 모두 비슷한 상황을 반영하고 있기 때문에 임의로 전파방해를 수행하는 RJS와 SUS기반의 PJS가 별반 다르지 않은 성능을 내는 것을 확인할 수 있다. 오히려 WCS가 SUS 기반의 PJS보다 좋은 성능을 보이는 것을 확인할 수 있다. 하지만 다음에 논의할 결과를 통해 비대칭 시나리오에서는 PJS도 충분히 효과적이라는 것을 확인할 수 있다.

그림 4는 비대칭 시나리오에서 사용자의 수를 변화시켜가며 평균 보안 전송률을 관찰한 결과이며, 총 두 명의 도청자($K = 2$)가 존재한다고 가정하였다. 대칭 시나리오의 결과(그림 3)와 비교했을 때 SUS기반의 PJS의 결과도 AJS의 결과(WUS 혹은 SUS)와 유사한 성능을 내는 것을 확인할 수 있다. SUS 기반의 PJS는 사용자 수가 적을 때는(1명 ~ 10명) 성능이 좋지 않지만 사용자 수가 많아지면서 높은 평균 보안 전송률을 달성하는 것을 확인할 수 있다. 비대칭 시나리오는 사용자와 도청자가 상대적으로 소형기지국에 근접한 위치에 존재하는 경우를 묘사한 것이다. 즉, SUS

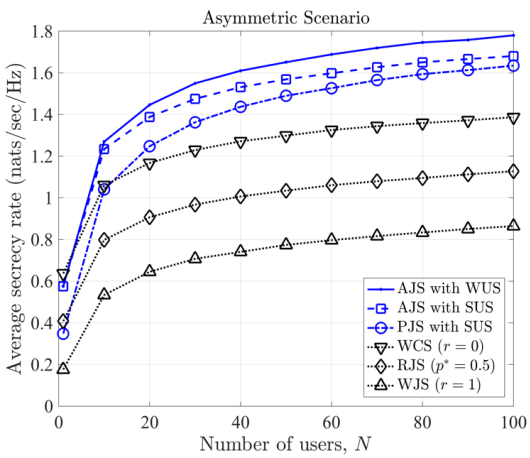


그림 4. 비대칭 시나리오에서 사용자 수에 따른 보안 전송률.
Fig. 4. Average secrecy rate vs. $N$ (asymmetric case).

기반의 PJS는 소형기지국에 가까이 위치하는 사용자를 위한 보안 통신 방법으로 상당히 효과적임을 이 결과로 확인할 수 있다. 본 논문에서 제안한 PJS는 도청자의 통계적 채널 정보만 활용했음에도 불구하고 좋은 성능을 보여준다. 따라서 PJS는 이종 망에서 소형기지국을 통해 활용할 수 있는 유용한 물리계층 보안 통신 방법 중에 하나라고 할 수 있다.

## Ⅵ. 결 론

본 논문에서는 이종 망에서 소형기지국을 물리계층 보안을 위해 활용할 수 있는 방안에 대해서 살펴보았다. 논문에서는 보안 전송률을 높일 수 있는 두 가지 사용자 선택 기준을 제시하였다: WUS, SUS.

더 나아가 사용자가 선택 되었을 때 소형기지국을 활용한 전파방해 전략을 제안하였다(AJS, PJS). 강한 채널 가정에서는 매 순간 정확한 전파방해를 수행하는 AJS을 제안하였고 약한 채널 가정에서는 확률적으로 전파방해는 수행하는 PJS를 제안하였다. 모의실험을 통해 PJS의 전파방해 확률에 대한 수학적 분석 결과를 확인하였으며 비대칭 시나리오에서는 도청자의 통계적 채널 정보만을 활용하는 PJS도 충분히 효과적이라는 것을 확인하였다. 마지막으로, 본 연구를 확장하여 하한(lower bound)을 활용한 최적화 문제 대신 본래의 최적화 문제를 분석하여 전파방해 전략을 제안하는 물리계층 보안 분야의 좋은 연구 주제가 될 것이다.

## References


[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, “The gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, Jul. 1978.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550-1573, Third Quarter, 2014.

[6] I. Bang, S. M. Kim, and D. K. Sung, “Effects of multiple antennas and imperfect channel knowledge on secrecy multiuser diversity,” *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1564 -1567, Sept. 2015.

[7] I. Bang, S. M. Kim, and D. K. Sung, “Secrecy multiuser diversity for distributed antenna systems from the perspective of user-scaling law,” in *Proc. IEEE ICC*, May 2016.

[8] I. Bang, B. C. Jung, and D. K. Sung, “A power control scheme for improving secrecy rate in multi-cell uplink networks,” *J. KICS*, vol. 42, no. 1, pp. 39-41, Jan. 2017.

[9] S. Goel and R. Negi, “Guaranteeing secerecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[10] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” *IEEE Trans. Veh. Tech.*, vol. 59, no. 8, pp. 3831-3842, Jul. 2010.

[11] Z. Ding, K. Leung, D. L. Goeckel, and D. Towsley, “Opportunistic relaying for secrecy communications: Cooperative jamming vs relay chatting,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725-1729, Jun. 2011.

[12] J. H. Lee, S. H. Chae, and W. Choi, “Opportunistic jammer selection for secure degrees of freedom,” in *Proc. IEEE GLOBECOM*, Dec. 2012.

[13] I. Bang, S. M. Kim, and D. K. Sung, “Opportunistic user selection with adaptive jamming for secure communication in heterogeneous networks,” in *Proc. IEEE PIMRC*, Sept. 2014.

[14] I. Bang, S. M. Kim, and D. K. Sung, “Artificial noise-aided user scheduling for optimal secrecy multiuser diversity,” *IEEE*

*Commun. Lett.*, vol. 21, no. 3, pp. 528-531, Mar. 2017.

[15] S. M. Kim and M. Bengtsson, "Virtual full-duplex buffer-aided relaying in the presence of inter-relay interference," *IEEE Tran. Wireless Commun.*, vol. 15, no. 4, pp. 2966-2980, Apr. 2016.

[16] X. Ge, H. Jin, J. Zhu, J. Cheng, and V. C. Leung, "Exploiting opportunistic scheduling in uplink wiretap networks," *IEEE Trans. Veh. Tech.*, vol. 66, no. 6, pp. 4886-4897, Jun. 2017.

[17] S. H. Chae, W. Choi, J. H. Lee, and T. Q. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Tran. Inf. Forensics and Secur.*, vol. 9, no. 10, pp. 1617-1628, 2014.

[18] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Area in Commun.*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[19] Athanasios Papoulis and S. Unnikrishna Pillai, *Probability, Random Variables and Stocahstic Processes,* New York, McGraw-Hill, 1984.

[20] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Seris, and Products,* Academic Press, 2003.

**방 인 규** (Inkyu Bang)

2010년 2월 : 연세대학교 전기전자공학부 학사

2012년 1월 : KAIST 전기및전자공학과 석사

2017년 8월 : KAIST 전기및전자공학과 박사

2017년 9월~현재 : 싱가포르 국립대학 컴퓨터과학과 박사후연구원

<관심분야> 무선통신, 시스템보안, 물리계층보안, 사물인터넷, 동시무선정보및전력전송, 항공기내통신

**김 수 민** (Su Min Kim)

2005년 2월 : 인하대학교 전자공학과 학사

2007년 2월 : KAIST 전기및전자공학과 석사

2012년 1월 : KAIST 전기및전자공학과 박사

2012년 1월~8월 : KAIST 정보전자연구소 박사후연구원

2012년 11월~2014년 10월 : 스웨덴왕립공과대학교 (KTH) 박사후연구원

2014년 11월~2015년 2월 : 스웨덴 에릭슨연구소 Experienced Researcher

2015년 3월~현재 : 한국산업기술대학교 전자공학부 조교수

<관심분야> 무선자원관리, 차세대이동통신, 협력중계통신, 기계타입통신, 물리계층보안, 통계적신호처리