논문 20-45-12-01 The Journal of Korean Institute of Communications and Information Sciences '20-12 Vol.45 No.12
https://doi.org/10.7840/kics.2020.45.12.2029

잠재적 도청에 대한 사용자 및 호의적인 재머 스케줄링 기법의 보안 성능 분석

방 인 규◆, 김 태 훈°

Secrecy Performance Analysis of Joint User and Friendly Jammers Scheduling Scheme against Potential Eavesdropping

Inkyu Bang◆, Taehoon Kim°

요 약

무선채널을 통해 데이터를 전달하는 무선통신 시스템은 근본적으로 도청 공격에 취약한 단점을 가진다. 따라서 본 논문에서는 상향링크 네트워크에서 잠재적 도청자가 존재하는 경우에 대비하여 데이터를 안전하게 전달하기 위한 사용자 스케줄링 기법을 제안하고 보안 성능을 분석한다. 그 결과로써 기존 연구 대비 다수의 호의적인 재머(전파 방해 기기)를 효과적으로 활용할 수 있는 개선된 스케줄링 기준과 호의적인 재머의 수가 1명이고 잠재적 도청자의 수가 1명 이상인 경우의 보안 중단 확률에 대한 수학적인 분석 방법을 새롭게 제시하고 모의실험을 통해 검증하였다.

키워드 : 물리계층 보안, 보안 중단 확률, 인공잡음, 잠재적 도청자, 기회적 사용자 스케줄링
Key Words : Physical-Layer Security, Secrecy Outage Probability, Artificial Noise, Potential Eavesdropper, Opportunistic User Scheduling

ABSTRACT

Wireless communication systems are vulnerable to eavesdropping attacks due to the broadcasting characteristics of wireless signals. Thus, in this paper, we propose a user scheduling criterion that selects users for data transmission and artificial noise in multiuser uplink networks with potential eavesdroppers. Compared with the previous studies, we propose a user scheduling criterion that allows multiple non-scheduled users to act as friendly jammers. In addition, we mathematically derive a secrecy outage probability of the proposed scheme in closed-form for the multiple eavesdroppers and only one friendly jammer condition and verify the results through simulations.

※ 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1F1A1069934).
※ 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1G1A1101176).
※ 이 논문의 일부는 한국통신학회 2020년도 하계종합학술발표회(20'.08.12~20'.08.14)에서 발표되었습니다.
◆ First Author : Hanbat National University Department of Information and Communication Engineering, ikbang@hanbat.ac.kr, 조교수, 정회원
° Corresponding Author : Hanbat National University Department of Computer Engineering, thkim@hanbat.ac.kr, 조교수, 정회원
논문번호 : 202008-181-A-RN, Received August 4, 2020; Revised October 11, 2020; Accepted November 2, 2020

Ⅰ. 서 론

오늘날 5세대 이동 통신(3GPP release 15), 와이파이 6(IEEE 802.11ax)으로 대표되는 차세대 무선통신 표준의 상용화와 함께 무선통신은 일상생활의 필수 요소로 자리 잡고 있다[1]. 그러나 무선채널을 통해 데이터를 전달하는 무선통신 시스템은 근본적으로 도청(eavesdropping) 공격에 취약한 단점을 가진다[2]. 실제로 무선 네트워크에 대한 다양한 도청 공격 사례가 보고되고 있으며, 2017년에는 무선랜(WLAN: wireless local area network) 환경에서 무선 신호에 대한 도청을 시작으로 무선 암호 프로토콜의 취약점을 발견한 연구가 발표되기도 하였다[3]. 따라서 무선 네트워크 보안을 주제로 하는 연구의 필요성이 더욱 대두되고 있다. 물리계층 보안(physical-layer security)은 정보이론 관점에서 무선 네트워크 보안을 연구하는 분야로써, 차세대 무선통신 시스템의 보안 문제 해결을 위해 주목 받고 있는 연구 분야 중 하나이다[4].

물리계층 보안에서는 기본적으로 송신기, 수신기, 도청자 등으로 구성되는 네트워크에서 수동적인 도청(passive eavesdropping) 공격이 발생하는 상황을 가정한다[5,6]. 그러나 최근 많은 논문이 다수의 송신기, 다수의 수신기, 다수의 도청자 등이 존재하는 다중 사용자 네트워크 환경에서 물리계층 보안 문제를 연구하기 시작하였다[7-9]. 예를 들어, 수신 안테나 및 사용자의 수와 보안 전송률(secrecy rate)의 관계를 분석하는 연구[7], 송신 전력조절이 보안 전송률에 미치는 영향을 분석하는 연구[8] 등이 발표되었다. 또한 2014년, 2019년 IEEE 통신 분야 조사 논문에서는 다중 사용자 네트워크 환경에서 물리계층 보안에 대한 전반적인 연구흐름 및 5G에서 보안 이슈 등이 발표되었다[9,10].

물리계층 보안에서 인공잡음(artificial noise)은 도청 공격을 효과적으로 방해하기 위해 의도적으로 재밍(jamming) 신호를 만들어내는 기술로 시스템의 보안성능(secrecy performance)을 높이기 위해 활용되는 대표적인 기술이다. 인공잡음을 생성하고 활용하는 방법은 2008년에 처음으로 논의되었으며[11], 이후 많은 논문들이 다중 안테나 혹은 중계기를 이용하여 인공잡음을 생성하고 분석하는 방법을 연구하였다[12,13]. 다중 안테나 혹은 중계기를 이용하여 인공잡음을 만들어 내는 방식과는 별도로, 다중 사용자 네트워크 환경에서 데이터 전송을 하지 않는 사용자를 호의적인 재머(friendly jammer)로 추가적으로 활용하여, 단일 안테나 상황에서도 인공잡음을 생성할 수 있는 사용자 스케줄링(user scheduling) 방법 또한 연구되고 있다[14,15]. 스케줄링 되지 않은 사용자를 추가적으로 활용하여 인공잡음을 생성하는 기존의 연구[14,15]는 도청자의 채널 정보에 대한 가정에 따라 해당 스케줄링 방식의 보안 전송률 또는 보안 중단 확률(secrecy outage probability)을 체계적으로 평가하고 분석하였다. 이러한 인공잡음 생성 기법은 안테나 수의 제약을 받지 않는 장점이 있지만 기존 연구는 도청자 수의 제약(오직 1명의 도청자를 가정), 호의적인 재머 수의 제약(오직 1명의 사용자를 활용), 제한적인 보안 성능 지표 분석(예: 보안 다양성 차수 분석) 등의 한계점을 역시 지니고 있다. 따라서 본 논문에서는 상향링크 네트워크에서 잠재적 도청자가 존재하는 경우에 대비하여 데이터를 안전하게 전달하기 위한 사용자 스케줄링 기법을 제안하고 보안 성능을 분석한다. 이 연구의 주요 기여도(contribution)는 다음과 같다.

① 기존 연구 결과[15]와 비교하여 1명 이상의 호의적인 재머를 효과적으로 활용할 수 있는 개선된 스케줄링 기준 제안하였다.

② 제한적인 기존의 분석 결과를 확장하여 호의적인 재머의 수가 1명이고 잠재적 도청자의 수가 1명 이상인 경우의 보안 중단 확률에 대한 수학적인 분석 결과를 새롭게 제시하였다.

③ 모의실험(simulation)을 통해 호의적인 재머 및 도청자의 수가 보안 중단 확률에 미치는 영향을 분석하였다.

논문은 총 5장으로 구성되어있으며 각 장의 내용은 다음과 같다. Ⅱ장에서는 이 연구에서 전제하는 시스템 모델과 보안 중단 확률의 개념을 설명한다. Ⅲ장에서는 추가적인 사용자 스케줄링을 통해 다수의 호의적인 재머를 선택하는 방법 제안하고 이와 관련한 수학적 결과를 도출한다. Ⅳ장에서는 모의실험을 통해 수학적 분석 결과를 검증하고 제안 스케줄링 방식의 성능을 평가한다. 마지막으로 Ⅴ장에서는 논의된 내용을 정리하며 최종 결론을 맺는다.

Ⅱ. 시스템 모델

이번 장에서는 문제 설정 및 분석을 위한 네트워크 모델을 설명하고 물리계층 보안에서 널리 쓰이는 보안 성능 척도(secrecy performance metric)를 소개한다.

2.1 잠재적 도청자가 존재하는 상향링크 네트워크

이 연구에서는 K명의 잠재적 도청자(potential eavesdropper)를 포함하는 총 N명의 사용자(즉, 송신

기)와 하나의 수신 기지국으로 구성된 다중 사용자 상향링크(uplink) 네트워크를 가정한다. 네트워크의 모든 구성 요소(즉, 사용자, 도청자, 기지국)는 하나의 안테나를 가지며, 도청자가 서로 협력 없이 독립적으로 사용자의 상향링크 신호를 엿듣는 상황을 가정한다[16]. 한 심벌 슬롯동안 $S+1$명의 사용자가 선택되며, 1명의 사용자는 데이터를 전송하고 나머지 S명의 사용자는 도청을 방해하기 위한 인공잡음을 생성한다.(사용자 스케줄링에 대한 자세한 소개는 3장에서 다룬다.) 예를 들어, 그림 1은 사용자가 7명($N=7$)이고 잠재적 도청자는 2명($K=2$)인 상황에서 데이터 전송을 위한 사용자(파란색 사용자) 1명을 선택하고 스케줄링되지 않은(unscheduled) 사용자(초록색 사용자) 1명을 추가적으로 선택($S=1$)하여 인공잡음을 생성하도록 했을 때, 데이터 신호와 간섭 신호의 영향을 보여준다. 또한 여기서 사용자와 수신기 사이의 무선링크는 '주요링크(desired link)', 사용자와 도청자 사이의 무선링크는 '도청링크(wiretap link)'로 지칭한다.

h_n, g_{nk}는 각각 n번째 사용자와 기지국 사이의 채널 계수($n\in\{1,\cdots,\mathrm{N}\}$), n번째 사용자와 k번째 잠재적 도청자 사이의 채널 계수($k\in\{1,\cdots,\mathrm{K}\}$)를 나타낸다. 각 채널 계수는 독립 가우시안(Gaussian) 분포를 따르는 레일리(Rayleigh) 페이딩 채널 모델을 가정한다. 즉, $h_n \sim CN(0,\sigma_{h_n}^2)$ 과 $g_{nk} \sim CN(0,\sigma_{g_{nk}}^2)$이 된다. 분석 편의성을 위해 모든 n과 k에 대하여 $\sigma_{h_n}^2=\sigma_h^2$와 $\sigma_{g_{nk}}^2=\sigma_g^2$을 가정한다[15]. 또한, 사용자 스케줄링에서 사용자와 기지국 사이의 순시 채널상태정보(instantaneous channel state information)는 이용 가능하지만 사용자와 도청자 사이에서는 순시 채널상태정보가 아닌 평균 채널 특성(즉, σ_g^2)만 이용할 수 있다고 가정한다. 또한 $S+1$명의 사용자 중에 잠재적 도청자가 선택되는 경우는 없다고 가정한다. 이러한 가정은 다른 연구에서도 이미 사용되고 있다[16].

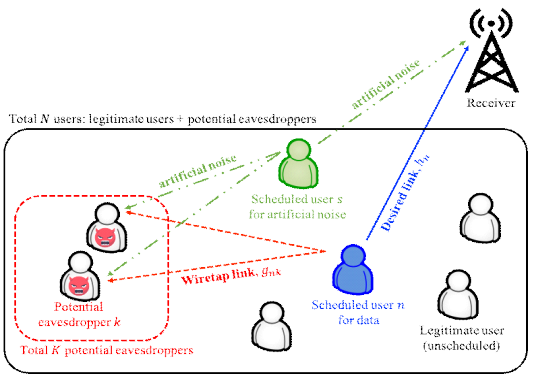

그림 1. 시스템 모델: 잠재적 도청자가 존재하는 다중사용자 상향링크 네트워크, $N=7$, $K=2$, $S=1$ 예시
Fig. 1. System model: multiuser uplink network with potential eavesdroppers, an example of $N=7$, $K=2$, $S=1$

2.2 보안 성능 척도

수식 표기의 편의를 위해 데이터 전송을 위해 선택되는 사용자 색인(index)은 u으로 표시하고 인공잡음 생성을 위해 선택된 사용자들의 색인은 s_m으로 표시한다($m\in\{1,\ldots,\mathrm{S}\}$). 이 때, 기지국과 k번째 잠재적 도청자의 수신 신호는 각각 다음과 같다.

$$y=h_u x_u+\sum_{m=1}^{S} h_{s_m}\delta_{s_m}+z, \tag{1-1}$$

$$y_k=g_{uk}x_u+\sum_{m=1}^{S} g_{s_m k}\delta_{s_m}+z_k, \tag{1-2}$$

여기서, x_u는 사용자 u가 전송하는 데이터 신호, δ_{s_m}는 사용자 u가 전송하는 인공잡음, z와 z_k는 기지국과 k번째 도청자의 수신 잡음을 각각 나타낸다.

사용자 u와 사용자 s_m의 송신 신호 대 잡음비(signal-to-noise ratio 또는 SNR)를 ρ로 표기할 때, 주요링크와 도청링크의 채널용량 차이로 정의되는 사용자 u의 보안 용량은 다음과 같다[6].

$$C(u)=\left[C_M(u)-C_W(u)\right]^+ \tag{2}$$

여기서 $[x]^+=\max\{x,0\}$을 나타내며 이는 도청링크의 채널용량이 주요링크의 채널용량보다 클 경우에는 보안 용량이 0이 되는 것을 표현해주기 위함이다. 또한 다중 사용자 네트워크를 전제하고 있기 때문에 적용되는 스케줄링 기법(즉, 선택되는 사용자)에 따라 주요링크와 도청링크의 채널용량이 달라진다. 따라서 주요링크와 도청링크의 채널용량 $C_M(u)$와 $C_W(u)$은 선택된 사용자 u의 함수로 각각 다음과 같이 표현할 수 있다.

$$C_M(u)=\log_2\left(1+\frac{\|h_u\|^2\rho}{\sum_{m=1}^{S}\|h_{s_m}\|^2\rho+1}\right), \tag{3-1}$$

$$C_W(u)=\log_2\left(1+\max_k\left\{\frac{\|g_{uk}\|^2\rho}{\sum_{m=1}^{S}\|g_{s_m k}\|^2\rho+1}\right\}\right), \tag{3-2}$$

수식 (3-2)에 최댓값을 고르는 연산자가 포함되는 이유는 도청자들이 독립적으로 행동한다는 가정 때문이다.

보안 용량은 물리계층 보안 연구에서 자주 쓰이는 보안 성능 척도이지만 정확한 계산을 위해서는 사용자와 도청자 사이의 순시 채널상태정보가 필요하다. 그러나 도청 순간에는 사용자와 도청자 사이의 채널 피드백 등이 존재하지 않기 때문에 순시 채널상태정보를 알아내는 것이 어렵다. 그 결과 스케줄링에서 사용자와 도청자 사이의 순시 채널상태정보를 사용할 수 없다고 가정하고 있으며 수식 (2)의 보안 용량 대신 보안 중단 확률이라는 성능 척도를 사용한다. 보안 중단 확률은 도청자의 순시 채널상태정보를 모를 때 보안 용량이 주어진 보안 전송률 R_0보다 작을 확률로 수학적 정의는 다음과 같다.

$$p_{so}(R_0) = \Pr\{C(u) < R_0\} = \Pr\{C(u) - C(u) < R_0\}. \quad (4)$$

Ⅲ. 추가적인 사용자 스케줄링을 통한 호의적인 재머 선택 방법

이번 장에서는 데이터 전송과 인공잡음 생성을 위해 $S+1$명의 사용자를 선택하는 기준(즉, 사용자 스케줄링 방법)을 제안한다. 또한 제안 스케줄링 기법의 보안 중단 확률을 수학적으로 도출한다.

3.1 보안 성능을 위한 호의적인 재머의 선택 기준

이 연구에서 분석하고자 하는 사용자 스케줄링 기법의 핵심 아이디어는 전체 N명의 사용자 중에서 데이터 전송을 위한 사용자 1명을 선택하고 나머지 $N-1$명이 사용자 중에 S명의 사용자를 선택하여 인공잡음을 생성하는 것이다(즉, 호의적인 재머의 역할). 제안하는 사용자 스케줄링 기법을 호의적인 재머와 사용자 통합 스케줄링(joint user and friendly jammers scheduling 또는 JUFS) 기법이라고 명명한다. 제안 기법은 기존 연구[14],[15]의 인공잡음 기반의 사용자 스케줄링(artificial noise aided user scheduling) 기법과 유사하지만, 도청자의 순시 채널상태정보에 대한 가정이 필요하지 않고 1명 이상의 호의적인 재머를 선택하여 스케줄링 할 수 있는 장점이 있다. 즉, 제안 기법은 인공잡음 기반의 사용자 스케줄링 기법을 일반화한 사용자 스케줄링 기법이다.

호의적인 재머와 사용자 통합 스케줄링 기법은 사용자와 도청자 사이의 순시 채널상태정보를 이용할 수 없기 때문에 사용자와 기지국 사이의 순시 채널상태정보만을 이용하여 $S+1$명의 사용자를 선택한다. 따라서 제안 기법은 사용자와 기지국 사이의 순시 채널이득(channel gain)이 가장 큰 사용자를 데이터 전송을 위해 선택하고 반대로 순시 채널이득이 가장 작은 S명의 사용자를 순서대로 선택하여 호의적인 재머의 역할(즉, 인공잡음 생성)을 수행하도록 한다. 이를 수식으로 나타내면 다음과 같다.

$$u = \arg\max_n \left\{ \| h_n \|^2 \right\}, \quad (5\text{-}1)$$

$$\{s_1, s_2, \ldots, s_S\} = \arg\min_{\pi \in \Pi(N_u, S)} \left\{ \sum_{m \in \pi} \| h_{s_m} \|^2 \right\}, \quad (5\text{-}2)$$

여기서 $\Pi(N_u, S)$는 전체 N명의 사용자 중 데이터 전송을 위해 선택된 사용자 u를 제외한 $N-1$명의 사용자 중 S명을 선택할 때 가능한 모든 조합의 순서쌍을 원소로 하는 집합이다. 즉, π는 S개의 색인 값을 포함하는 집합이다. 수식 (5-2)는 기지국과의 채널이득이 가장 작은 S명의 사용자 색인의 집합이다.

3.2 제안 스케줄링 기법의 보안 중단 확률 분석

호의적인 재머와 사용자 통합 스케줄링 기법의 보안 성능에 대한 수학적 분석과 평가를 위해, 일반적인 변수 값(즉, $N-1 \geq S \geq 1$, $K \geq 1$)에 대한 보안 중단 확률의 수학적 도출이 필요하다. 그러나 $S>1$인 경우, 수식 (5-1), (5-2)의 조건을 만족하는 수식 (3-1), (3-2)의 확률분포를 구하는 과정이 매우 복잡하고 어렵기 때문에 본 논문에서는 $S=1$, $\rho \to \infty$ 경우에 한하여 제안 기법의 보안 중단 확률을 수학적으로 도출한다.

제안 기법의 보안 중단 확률 분석을 위해서는 우선 수식 (5-1), (5-2)의 조건을 만족하는 수식 (3-1), (3-2)의 확률분포를 구해야 한다. $S=1$, $\rho \to \infty$일 때 수식 (3-1), (3-2)은 다음과 같이 표현할 수 있다.

$$C_M(u) = \log_2\left(1 + \frac{\| h_u \|^2}{\| h_s \|^2}\right), \quad (6\text{-}1)$$

$$C_W(u) = \log_2\left(1 + \max_k \left\{ \frac{\| g_{uk} \|^2}{\| g_{sk} \|^2} \right\}\right). \quad (6\text{-}2)$$

분석의 편의를 위해 수식 (6-1), (6-2)에 포함되어 있는 확률 변수의 조합을 다음과 같이 표기한다,

$$Z=\frac{\|h_u\|^2}{\|h_s\|^2},\quad W=\max_k\left\{\frac{\|g_{uk}\|^2}{\|g_{sk}\|^2}\right\}. \tag{7}$$

사용자 색인 u와 s는 수식 (5-1), (5-2)의 조건을 기준으로 선택되기 때문에, 확률변수 Z의 $\|h_u\|^2$는 N개의 지수 확률변수 중 최댓값을 나타내는 확률 변수이며 반대로 $\|h_s\|^2$는 N개의 지수 확률변수 중 최솟값을 나타내는 확률 변수가 된다. 두 확률변수 $\|h_u\|^2$, $\|h_s\|^2$의 함수로 표현되는 확률변수 Z의 누적분포함수(cumulative distribution function)는 기존 연구[15], 확률이론[17], 이항정리[18] 등을 이용하여 다음과 같이 구할 수 있다,

$$F_Z(z)=\sum_{i=0}^{N}\binom{N}{i}\frac{(-1)^i N}{iz+N}. \tag{8}$$

비슷한 방식으로 확률변수 W의 누적분포함수를 구할 수 있다. 단, 수식 (7)의 확률변수 W에서 $\|g_u\|^2$와 $\|g_s\|^2$의 확률 분포는 사용자 선택과 무관하기 때문에, $\|g_u\|^2$, $\|g_s\|^2$는 지수 확률변수가 된다. 또한 기존 연구[15]와 다르게 $K\geq 1$명의 도청자를 가정하기 때문에 확률변수 W는 확률변수 $\frac{\|g_{uk}\|^2}{\|g_{sk}\|^2}$의 최댓값을 나타내는 확률변수가 된다. 따라서 확률변수 W의 누적분포함수는 다음과 같다.

$$\begin{aligned}F_W(w)&=\left(1-\frac{1}{w+1}\right)^K\\&=\sum_{m=0}^{K}\binom{K}{m}\left(-\frac{1}{w+1}\right)^m,\end{aligned} \tag{9}$$

여기서 첫 번째 등식의 지수 K는 확률변수의 최댓값을 구하는 과정에서 유도된 결과이며 두 번째 등식은 이항정리의 적용 결과이다.

수식 (8), (9)와 두 확률변수에 관한 확률이론[17]을 적용하면 제안 기법의 보안 중단 확률을 다음과 같이 구할 수 있다.

$$\begin{aligned}p_{so}(R_0)&=\Pr\{\log_2(1+Z)-\log_2(1+W)<R_0\}\\&=\Pr\left\{\frac{1+Z}{1+W}<2^{R_0}\right\}\\&=\Pr\left\{Z<2^{R_0}(W+1)-1\right\}\\&=\int_0^{\infty}\int_0^{2^{R_0}(w+1)-1}f_Z(z)dz f_W(w)dw,\\&=\int_0^{\infty}F_Z\left(2^{R_0}(w+1)-1\right)f_W(w)dw,\end{aligned} \tag{10}$$

여기서 $f(z)$, $f(w)$은 각각 확률변수 Z와 W의 확률분포함수(probability density function)이며, $f(w)$의 구체적인 형태는 수식 (9)의 결과를 미분하여 얻을 수 있다.

수식 (10)의 계산 과정은 다음과 같다.

$$\begin{aligned}&p_{so}(R_0)\\&=\int_0^{\infty}F_Z\left(2^{R_0}(w+1)-1\right)f_W(w)dw\\&=\int_0^{\infty}\sum_{i=0}^{N}\lambda_i\left(\frac{1}{\alpha_i w+1}\right)\sum_{m=1}^{K}\theta_m\left(\frac{1}{w+1}\right)^{m+1}dw\\&=\sum_{i=0}^{N}\sum_{m=1}^{K}\lambda_i\theta_m\int_0^{\infty}\left(\frac{1}{\alpha_i w+1}\right)\left(\frac{1}{w+1}\right)^{m+1}dw,\end{aligned} \tag{11}$$

여기서 λ_i, θ_m, α_i 수식 표기의 편의를 위해 정의했으며, $\lambda_i=\binom{N}{i}\frac{(-1)^i N}{i2^{R_0}-i+N}$, $\theta_m=\binom{K}{m}(-1)^{m+1}m$, $\alpha_i=\frac{i2^{R_0}}{i2^{R_0}-i+N}$을 각각 나타낸다.

수식 (11)의 두 번째 등식에 포함되어 있는 적분은 기존 적분표[19]의 결과(3.197.5)를 이용하면 계산할 수 있다. 따라서 $S=1$, $\rho\to\infty$일 때 JUFS 기법의 보안 중단 확률은 최종적으로 다음과 같다.

$$\begin{aligned}&p_{so}(R_0)\\&=\sum_{i=0}^{N}\sum_{m=1}^{K}\lambda_i\theta_m B(1,m+1)\,{}_2F_1(1,1;m+2;1-\alpha_i),\end{aligned} \tag{12}$$

여기서 λ_i와 θ_m는 수식 (11)에서 정의되어 있으며, $B(x,y)$는 베타함수(beta function), ${}_2F_1(a,b;c;z)$는 초기하함수(hypergeometric function)를 의미한다[14]. 베타함수와 초기하함수는 공학 분야에서 널리 활용되는 함수로 정의는 각각 다음과 같다.

$$B(x,y)=\int_0^1 t^{x-1}(1-t)^{y-1}dt, \tag{13-1}$$

$${}_2F_1(a,b;c;z)=\sum_{n=0}^{\infty}\frac{a^{\bar{n}}b^{\bar{n}}}{c^{\bar{n}}}\frac{z^n}{n!}, \tag{13-2}$$

여기서 $a^{\bar{n}}$은 상승계승(rising factorial)을 나타내며 다음과 같이 계산할 수 있다.

$$a^{\bar{n}} = \begin{cases} 1 & n=0, \\ a(a+1)\cdots(a+n-1) & n>0. \end{cases} \quad (14)$$

수식 (12)의 베타함수와 초기하함수는 MATLAB을 포함하는 많은 분석용 소프트웨어에 내장 함수로 구현되어 있기 때문에 어렵지 않게 함수 값을 계산할 수 있다. 결과적으로, 수식 (12)는 $S=1$, $\rho\to\infty$의 제약 조건하에서 일반적인 도청자 수($K\geq 1$)에 대한 제안 기법의 보안 중단 확률을 수학적/수치적으로 분석할 수 있는 중요한 결과이다. 수식 (12)에 대한 검증과 제안 기법의 보안 성능에 대한 모의실험 결과는 다음 장(4장)에서 구체적으로 논의한다.

Ⅳ. 성능 평가

이 장에서는 호의적인 재머와 사용자 통합 스케줄링(JUFS) 기법의 보안 중단 확률을 분석한다. 모의실험을 통해 수식 (12)의 정확성을 확인하고 제안 기법의 보안 중단 확률을 시스템의 변수 값을 바꿔가며 다른 기법과 비교 분석한다.

제안 기법의 성능을 분석하기 위해 MaxSNR과 MaxRnd으로 명명되는 두 가지 기법을 참고한다. MaxSNR 기법은 호의적인 재머를 선택하지 않고(즉, $S=0$) 데이터 전송을 위한 사용자 한 명을 선택하는 사용자 스케줄링 기법이다. 즉, MaxSNR 기법은 데이터 전송을 위해 매 전송슬롯마다 기지국과의 순시 채널상태정보가 가장 좋은 사용자를 선택한다. 추가로 MaxRnd 기법은 데이터를 전송하는 사용자는 MaxSNR 기법과 동일하게 선택하고 추가로 S명의 사용자를 무작위로 선택하여 도청을 방해하기 위한 호의적인 재머로 활용하는 사용자 스케줄링 기법이다. 제안(JUFS) 기법, MaxSNR 기법, MaxRnd 기법 간의 동일한 평균 송신전력 조건을 보장하기 위해서, MaxSNR 기법에서 선택된 사용자는 매 전송슬롯 마다 P의 전력을 소비하고 제안(JUFS) 기법과 MaxRnd 기법에서 선택된 사용자(데이터 또는 호의적인 재머)는 매 슬롯 $\frac{P}{S+1}$의 전력을 소비하는 것을 가정한다.

그림 2는 SNR 변화에 따른 제안(JUFS) 기법의 보안 중단 확률을 나타낸다. 기본적인 시스템 변수는 각각 $S=1$, $K=2$, $R_0=1.5$ bps/Hz으로 설정하였고, $N=10$, $N=20$의 두 경우에 대하여 수식 (12)의 결과와 모의실험의 결과를 비교하였다. $S=1$, $\rho\to\infty$일 때, 보안 중단 확률을 나타내는 수식 (12)의 결과와 모의실험의 결과가 정확하게 일치하는 것을 확인할 수 있다. 앞서 3장에서 논의한 바와 같이 수식 (12)에 포함되어 있는 베타함수와 초기하함수의 계산은 수치분석용 소프트웨어(MATLAB)를 활용하였다.

그림 3는 SNR 변화에 따른 제안(JUFS) 기법의 보안 중단 확률을 나타낸다. 기본적인 시스템 변수는 각각 $K=2$, $R_0=2.0$ bps/Hz으로 설정하였다. 사용자 수와 호의적인 재머의 수에 대한 효과를 관찰하기 위해 $N=50$, $N=100$, $S=1$, $S=3$인 경우(각 변수의 조합)에 대한 모의실험을 진행하였다. 제안 기법($N=50$, $S=1$)과 MaxSNR 기법($N=50$)의 결과를 비교해 보면, 호의적인 재머를 위해 사용자를 추가로 한 명만 선택하더라도 보안 중단 확률 관점에서 상당

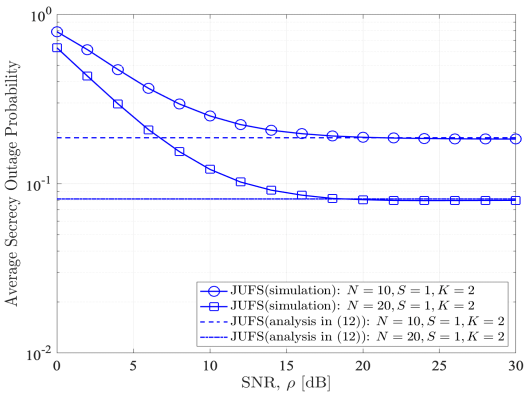

그림 2. $R_0=1.5$ bps/Hz일 때 SNR 변화에 따른 JUFS 기법의 보안 중단 확률: (12)의 결과와 수치적 결과 비교
Fig. 2. Average secrecy outage probability for varying SNR when $R_0=1.5$ bps/Hz (comparison between analytical result in (12) and numerical result)

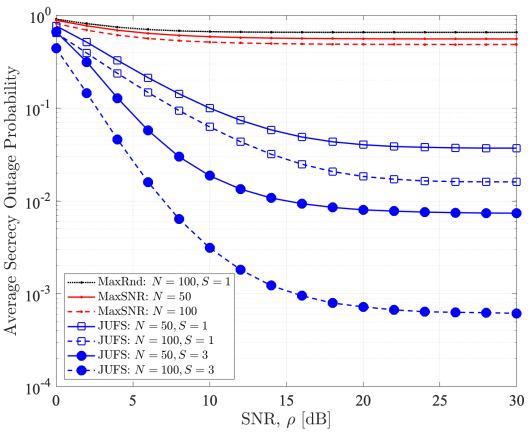

그림 3. $R_0=2.0$ bps/Hz일 때 SNR 변화에 따른 JUFS 기법의 보안 중단 확률: 참고 기법들과의 성능 비교
Fig. 3. Average secrecy outage probability for varying SNR when $R_0=2.0$ bps/Hz (comparison with MaxSNR and MaxRnd schemes)

한 성능 이득이 발생하는 것을 확인할 수 있다. 또한 제안 기법은 사용자 수 증가에 따른($N=50\rightarrow100$) 성능 증가 폭이 MaxSNR 기법보다 우수한 것을 확인할 수 있다. MaxRnd 기법의 결과를 통해 무작위로 선택한 호의적인 재머는 오히려 보안 성능 악화를 초래한다는 것을 확인할 수 있으며, 이를 통해 제안 기법과 같은 호의적인 재머 선택의 기준이 필요하다는 것을 확인할 수 있다. 제안 기법에서 호의적인 재머의 수(S)의 증가는 보안 성능 향상으로 이어지며 사용자 수(N)가 많을 때 성능 증가 폭이 더욱 커지는 것을 확인할 수 있다.

그림 4는 도청자 수(K)의 변화에 따른 제안(JUFS) 기법의 보안 중단 확률을 나타낸다. 기본적인 시스템 변수는 각각 $N=50$, $R_0=1.0$ bps/Hz, $\rho=30$ dB으로 설정하였다. K 값이 증가할 경우 사용자와의 무선 채널 상태가 좋은 도청자가 존재할 확률이 증가하기 때문에, 모든 기법의 보안 중단 확률이 증가한다. 제안 기법은 모든 K값의 범위에서 다른 기법에 비해 우수한 성능을 보인다.

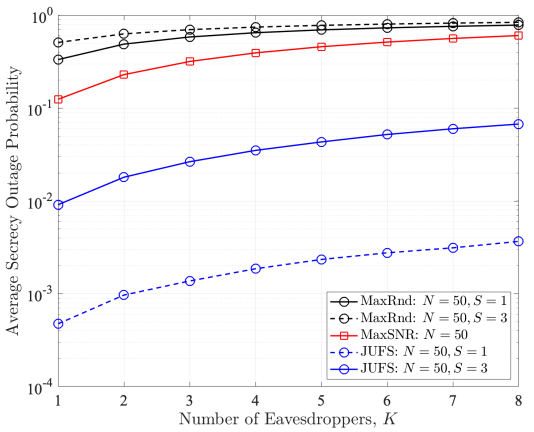

그림 4. $R_0=1.0$ bps/Hz일 때 도청자 수 K의 변화에 따른 JUFS 기법의 보안 중단 확률: 참고 기법들과의 성능 비교
Fig. 4. Average secrecy outage probability for varying K when $R_0=1.0$ bps/Hz (comparison with MaxSNR and MaxRnd schemes)

V. 결 론

본 논문에서는 잠재적 도청자가 존재하는 다중 사용자 네트워크에서 보안 성능(보안 중단 확률)을 높이기 위한 데이터 전송 및 호의적인 재머 선택 기준을 제안하였다. 호의적인 재머와 사용자 통합 스케줄링 (JUFS) 기법은 매 전송슬롯마다 데이터 전송을 하지 않는 사용자 중 일부를 호의적인 재머로 활용하여 효과적으로 보안 중단 확률은 낮추는 사용자 스케줄링 기법이다. 제안 기법의 보안 중단 확률을 수학적으로 분석하고 그 결과를 모의실험을 통해 검증하였다. 또한 다양한 시스템 변수 값에 대한 모의실험을 진행하여 각 변수 값이 제안 기법의 보안 중단 확률에 미치는 영향을 분석하였다. 연구 결과를 토대로 호의적인 재머의 수(S)와 도청자 수(K)의 조건에 따라 제안 기법을 다양한 시나리오에 적용할 수 있을 것으로 기대된다. 마지막으로, 연구의 주요 결과인 수학적 결과를 좀 더 일반적인 경우로 확장하는 것은 물리계층 보안 분야의 좋은 연구 주제가 될 수 있다.

References

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 3, pp. 1617-1655, Third Quarter 2016.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," in *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[3] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM Conf. Comput. and Commun. Secur.*, pp. 1313-1328, 2017.

[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things J.*, vol. 6, no. 5, pp. 8169-8181, May 2019.

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

[6] 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.

[7] 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, Sep. 2015.

[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] 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. Surv. Tuts.*, vol. 16, no. 3, pp. 1550-1573, Third Quarter, 2014.

[10] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 4, pp. 3682-3722, Forth Quarter, 2019.

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

[12] 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.

[13] 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 Trans. Inf. Forensics and Secur.*, vol. 9, no. 10, pp. 1617-1628, 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] I. Bang, S. M. Kim, and D. K. Sung "Artificial noise-aided user scheduling from the perspective of secrecy outage probability," *IEEE Trans. Vech. Tech.*, vol. 67, no. 8, pp. 7816-7820, Aug. 2018.

[16] I. Bang and B. C. Jung, "Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers," *IEEE Access*, vol. 7, pp. 127078-127089, Sep. 2019.

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

[18] J. L. Coolidge, "The story of the binomial theorem," *The Am. Math. Monthly*, vol. 56, no. 3, pp. 147-157, Mar. 1949.

[19] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Seris, and Products*, London, UK: Academic Press, 2003.

방 인 규 (Inkyu Bang)

2010년 2월 : 연세대학교 전기전자공학부 (공학사)
2012년 1월 : 한국과학기술원 전기및전자공학과 (공학석사)
2017년 8월 : 한국과학기술원 전기및전자공학부 (공학박사)
2017년 9월~2019년 2월 : 싱가포르 국립대학 컴퓨터과학과 박사후연구원
2019년 3월~2019년 7월 : 국방과학연구소 지상기술연구원 선임연구원
2019년 8월~현재 : 한밭대학교 정보통신공학과 조교수
<관심분야> Wireless Network Security, Physical-Layer Security, 5G/IoT, SWIPT, UAV, Machine Learning, Deep Learning
[ORCID:0000-0001-7109-1999]

김 태 훈 (Taehoon Kim)

2011년 2월 : 한양대학교 정보통신공학부 (공학사)
2013년 2월 : 한국과학기술원 전기및전자공학과 (공학석사)
2017년 8월 : 한국과학기술원 전기및전자공학부 (공학박사)
2017년 9월~2020년 2월 : 국방과학연구소 국방첨단기술연구원 선임연구원
2020년 3월~현재 : 한밭대학교 컴퓨터공학과 조교수
<관심분야> Wireless Communications, 5G/IoT, Multiple Access Systems, Physical-Layer Security, Machine Learning, Reinforcement Learning
[ORCID:0000-0002-9353-118X]