

A Security-Aware Uplink Power Allocation Technique in IEEE 802.11ax WLANs

Hyunju Park[†] · Wonjun Lee^{†*}

ABSTRACT

With the advancement of wireless communication technologies, modern WLAN systems enable flexible data transmission through wireless networks. The latest Wi-Fi 6 and Wi-Fi 7 standards significantly improve speed, efficiency, and connectivity, making them suitable for applications in smart homes, industrial IoT, and densely populated environments. However, current WLAN security mainly relies on cryptographic key-based methods based on Shannon's security model, which may not be sufficient in the approaching quantum cryptography era. In this paper, we propose a technique to enhance security by leveraging the multi-resource features of OFDMA, a key element introduced in the latest WLAN standards. Our method leverages artificial multi-user interference among legitimate users without adding extra interfering sources, thus reducing the effectiveness of eavesdropping. This study is the first to discuss power allocation for enhancing security in the OFDMA uplink. It holds practical significance by proposing a power allocation technique for uplink security while considering the standards outlined in IEEE 802.11ax. We introduce an algorithm that adjusts resource allocation and power to intentionally create interference in secure communication channels. Performance evaluations using SDR equipment show that the proposed approach improves security, as demonstrated by enhancements in bit error rate and security rate compared to well-known power allocation algorithms.

Keywords : IEEE 802.11ax, WLAN, OFDMA, Physical Layer Security, Multi User Interference

IEEE 802.11ax 무선랜에서의 상향링크 보안성 향상을 위한 전력할당 기법

박 현 주[†] · 이 원 준^{†*}

요 약

무선랜(WLAN)은 무선 매체를 이용하여 유연하게 데이터 통신을 수행할 수 있는 시스템으로, 최신 Wi-Fi 6, Wi-Fi 7 표준은 높은 속도, 효율성, 연결성을 증대시켜 스마트홈, 산업용 IoT, 사용자 밀집 환경에서 사용자 편의를 높이는 데 기여하고 있다. 현재 무선랜 보안은 Shannon의 보안 모델에 주로 의존하는 암호화 키 기반 공유 접근 방식에 의존하고 있지만, 암호화 기반 보안 기법은 해독 위험이 존재하고, 이에 대비하여 암호 기반 보안 방식 외의 대안이 필요한 실정이다. 본 논문에서는 최신 무선랜 표준에서 도입된 OFDMA의 다중 자원 특성을 활용하여 추가적인 간섭 생성 주체 없이 결합된 사용자들만으로 다중 사용자 간섭을 발생시켜 도청 채널을 저하시킬 수 있는 기술을 제안한다. 본 연구는 OFDMA 상향링크에서의 보안성 향상을 위한 전력할당을 처음으로 논의하는 연구로, IEEE 802.11ax에서의 실제 표준을 고려하여 상향링크 보안을 위한 전력할당 기법을 제안함에 있어 실질적인 의미를 가진다. 제안된 기술은 기밀 통신을 수행하는 자원 단위에 의도적으로 다중 사용자 간섭을 발생시키기 위해 자원 단위 및 전력을 할당하고, 이를 조정하는 알고리즘으로 구성된다. 본 논문에서는 SDR 장비를 사용하여 제안 기술의 성능을 실험 및 평가하고, 기존에 잘 알려진 전력할당 알고리즘과 비교하여 도청자의 비트 에러율과 보안율을 분석한다.

키워드 : IEEE 802.11ax, WLAN, OFDMA, 물리계층보안, 다중 사용자 간섭

※ 이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2024-00338786)과 정보통신기획평가원의 지원(No. RS-2023-00234719, (SW스타랩) 서비스 연속성 지향 예지 Continuum SW 프레임워크)을 받아 수행된 연구임.

[†] 준 회 원 : 고려대학교 정보보호대학원 석사과정

^{†*} 종신회원 : 고려대학교 정보보호대학원 교수

Manuscript Received : October 28, 2024

First Revision : December 18, 2024

Accepted : January 10, 2025

*Corresponding Author : Wonjun Lee(wlee@korea.ac.kr)

1. 서 론

무선 네트워크 신호는 브로드 캐스트 특성으로 인해 잠재적인 도청자에 의해 도청될 수 있다. 특히 WLAN 환경은 다양한 사용자가 비교적 쉽게 접근 가능한 공개된 무선망이기 때문에 무선 네트워크에 대한 보안 방안이 필수적으로 적용되어야 한다. IEEE 802.11 표준에서는 도청 공격으로부터 안전하도록 WPA2 및 WPA3 기법으로 무선 네트워크 신호를 암호화한다. 그러나 이와 같은 보안 기법은 Shannon의 보안 모델에 기반한 암호화 키 기반 공유 접근 방식에 의존하며, 이를 보완하는 대안으로 물리계층 보안 기법이 혁신적인 개념으로 주목받고 있다[1].

물리계층 보안 기법은 암호화 키 기반 기법에 대한 대안적 기술로서 정보이론에 기초하며 물리매체의 고유한 임의성 및 적법한 채널과 도청 채널 간의 차이를 활용하여 무선 네트워크 신호를 잠재적인 도청자로부터 보호한다[2]. 해당 보안 기법의 특징은 컴퓨팅 능력에 의존하지 않으므로 그 복잡성이 낮고 자원을 절약할 수 있는 이점을 제공하여 암호화 키 기반 공유 접근 방식에 의존하지 않고 효과적인 보완 기법으로 사용될 수 있다.

현재 상용화된 4G, 5G 및 802.11ax, 802.11 be 등의 표준은 효율적인 채널 사용을 위해 OFDMA(orthogonal frequency-division multiple access)를 도입했다. 본 논문에서는 해당 OFDMA 방식의 다중-자원 특성을 활용하여 상향링크 통신에서의 보안성 향상을 위한 트리거 기반 송신전력 조정 기법을 제안한다. 잠재적 도청자의 공격 모델은 세 가지 조건으로 가정하였으며, 본 연구진은 도청자의 채널 상태를 악화시키기 위해 다중 사용자 간섭(multi-user interference, MUI)을 의도적으로 유도하는 상향링크 송신 전력 할당기법을 제안한다. 본 연구는 IEEE 802.11ax 표준을 고려하여 OFDMA 상향링크의 보안을 향상시키기 위한 전력할당 기법을 최초로 제안하였으며, 각 위협 모델에서 제안 기법의 보안성을 평가하기 위해 SDR 장비를 이용하여 실험하였다. 실험 결과, 각 공격 모델에서 도청자의 비트 오류율은 45%, 50.2%, 25.6%에 도달하였으며, 이에 따라 제안 기법의 보안성 향상을 입증하였다.

2. 배경지식 및 관련연구

본 장에서는 IEEE 802.11ax에서의 OFDMA 기반 상향링크 통신 방식 및 다중 사용자 간섭에 대한 배경지식과 관련 연구에 대해 소개한다.

2.1 IEEE 802.11ax OFDMA 상향링크 통신 및 자원할당 방식

OFDMA 방식은 주파수, 시간, 전력을 사용자별로 할당할 수 있는 방식으로, IEEE 802.11ax는 자원단위(resource unit, RU)를 이용하여 각 사용자에게 할당한다. IEEE 802.11ax에서

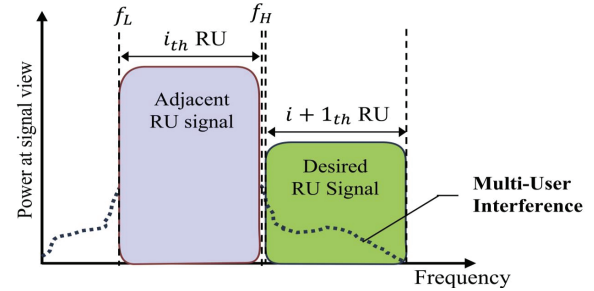


Fig. 1. Impact of Multi-User Interference from adjacent RU

의 상향링크 통신 방식은 각 STA들이 AP로부터 수신한 트리거 프레임의 기반으로 전송을 수행한다. 본 연구는 다중 사용자 간섭을 의도적으로 발생시킬 수 있도록 할당된 전력을 자원 할당 메커니즘을 이용하여 각 STA에 할당한다. 해당 메커니즘은 AP가 STA의 송신전력을 조정할 수 있도록 일련의 절차를 제공하는데, AP는 트리거 프레임에 STA 별 정보 필드에 AP의 신호세기 값 TX_{power}^{AP} 과 수신 받고자 하는 신호세기 값 $Target_{RSSI}$ 를 포함하여 전달한다. STA는 해당 값에 따라 송신 전력을 조정하며, AP는 이를 통해 중앙에서 STA 들의 송신 전력을 제어할 수 있다[4].

2.2 다중 사용자 간섭의 영향

OFDMA 시스템은 주파수 차원에서 부반송파를 각 사용자에게 할당하며, 부반송파 간 간섭을 방지하기 위해 부반송파 직교성이 보장되어야 한다. 그러나 상향링크 통신에서 STA들은 각기 다른 CFO(carrier frequency offset), 전력 한계, 채널 상태로 인해 ICI(inter carrier interference)가 발생하며, 전력 차이가 클 경우 강한 신호가 약한 신호에 상당한 간섭을 발생시킨다. 이러한 간섭을 다중 사용자 간섭이라고 한다.

Fig. 1은 인접하는 자원단위로부터 발생한 다중 사용자 간섭이 요구하는 자원단위에 미치는 영향을 나타낸다. 본 논문은 이러한 다중 사용자 간섭을 의도적으로 발생시킬 수 있는 자원단위 및 전력 할당을 위한 Three-step 기법을 제안하여 도청자의 디코딩 실패를 유도하는 동시에 정당한 수신자는 정상적으로 디코딩이 가능하도록 한다. 인접한 자원단위로부터 발생한 총 다중 사용자 간섭 전력은 수식 1과 같이 모델링된다. 인접한 두 자원단위 중 전력이 상대적으로 낮은 자원단위의 채널은 전력 차 크기가 클수록 총 다중 사용자 간섭 전력이 증가하고, 이에 따라 신호 대 잡음 비(signal-to-noise ratio, SNR)가 저하된다. 자원단위 집합 S 중 i 번째로 위치하는 RU_i 가 존재할 때, $RU_{i \pm 1}$ 의 전체 부반송파로부터 RU_i 의 전체 부반송파에 미치는 다중 사용자 간섭 전력 $M_{i \pm 1}$ 은 다음과 같이 표현될 수 있다[11].

$$M_{i \pm 1} = \frac{P^{i \pm 1}}{P^i} \left(\frac{f_{i \pm 1}}{\Delta f} \right)^2 \sum_{l=1}^{N_i} \sum_{j=1}^{N_{ij}} \frac{1}{(l+j+g-1)^2} \quad (1)$$

위 수식에서 N_i , $N_{i\pm 1}$ 는 RU_i 와 $RU_{i\pm 1}$ 의 전체 부반송파 집합을 나타내고, $P^i = E[S^i]^2$, $P^{i\pm 1} = E[S^{i\pm 1}]^2$ 는 각각 RU_i 와 $RU_{i\pm 1}$ 의 심볼의 평균 신호 전력을 나타낸다. $f_{i\pm 1}$ 는 $RU_{i\pm 1}$ 의 캐리어 주파수 오류(carrier frequency offset, CFO)를 나타내며, 본 연구에서는 캐리어 주파수 오류를 사전보상 후에도 발생할 수 있는 잔여 CFO로 $\{-1.5, 1.5\}$ kHz 범위 내로 가정한다. g 는 자원단위 간 가드 부반송파 수를 나타낸다. Δf 는 주파수 간격을 나타내며 78.125 kHz 이다. 위 수식에 따라 다중 사용자 간섭 전력 영향을 받은 RU_i 의 SINR과 각 구성 요소별 수신 신호는 다음과 같이 표현될 수 있다.

$$\begin{aligned} \text{SINR}_i &= 10\log_{10} \left(\frac{\sum_{l=1}^{N_i} E_l^i}{N_i} \right) / (M_{i\pm 1} + w_i) \\ y_i^r(n) &= \left(\sum_{l=1}^{N_i} x_{i,l}^r H_{i,l}^r + w_{i,l}^r \right) + \underbrace{M_{i\pm 1}^r(n)}_{\text{interference}} \\ y_i^e(n) &= \left(\sum_{l=1}^{N_i} x_{i,l}^e H_{i,l}^e + w_{i,l}^e \right) + \underbrace{M_{i\pm 1}^e(n)}_{\text{interference}} \end{aligned} \quad (2)$$

$E_l^i = E[S_{i,l}^i]^2$ 는 RU_i 의 l 번째 부반송파로 전송된 전체 심볼의 평균 전력이며, w_i 은 RU_i 의 AWGN 잡음 전력을 나타낸다. $y_i^r(n)$, $y_i^e(n)$ 는 AP와 도청자가 각각 수신한 RU_i 의 n 번째 심볼 신호이고, $x_{i,l}^r$, $x_{i,l}^e$ 은 RU_i 의 $l \in L_i$ 번째 부반송파로 수신된 신호, L_i 는 RU_i 의 부반송파 집합, $H_{i,l}^r$, $H_{i,l}^e$ 은 STA와 각 구성요소 간의 채널신호, $w_{i,l}^r$, $w_{i,l}^e$ 은 RU_i 의 l 번째 부반송파의 AWGN 잡음 전력, $M_{i\pm 1}^r(n)$, $M_{i\pm 1}^e(n)$ 은 $RU_{i\pm 1}$ 으로부터 RU_i 에 미치는 총 다중 사용자 간섭을 나타낸다.

2.3 OFDMA 기반 무선시스템의 보안성 향상 관련 연구

OFDMA 무선 시스템에서의 다양한 물리계층 보안 기법 중 다중-차원 특성을 활용한 자원 할당 기법은 자원단위 및 전력을 보안성 향상 요구에 따라 유연하게 할당할 수 있다[5-10]. [5]은 OFDMA 시스템에서의 랜덤한 서브채널 할당 방식과 균일한 송신전력 할당 방식은 전체 보안 성능을 저하시킴을 보였으며, 이로부터 자원 할당 문제와 물리계층 보안을 통합하는 데에 주목하기 시작하였다. [6]는 비밀률(secret rate)의 최대화를 목적으로 전력 및 부반송파 할당 최적화의 초기 시도를 보였으며, [7]는 기밀한 통신을 수행하는 사용자들의 비밀률을 보장할 수 있는 서브채널 및 전력 할당 기법을 제안함으로써 OFDMA 하향링크에서 non-zero 비밀률을 달성함을 보였다. [8]은 OFDMA 시스템에서 자원을 할당할 때, 오직 보안성 향상만을 목적으로 최적화함으로써 모든 사용자의 비밀률을 최대화 하고 사용자 간 비밀률의 균형 또한 보장될 수 있도록 하였다. [9]은 유일하게 OFDMA 상향링크에서 보안성 향상을 위한 자원단위 할당을 제안하였으나, 전 이중방식 시

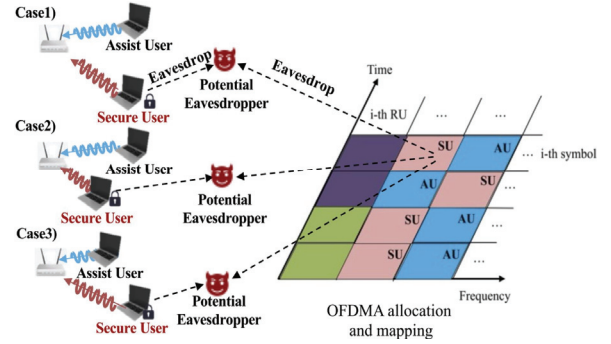


Fig. 2. Eavesdrop attack model on confidential signal

스템에서 빔포밍을 이용해 방향성을 가진 잡음을 생성하는 기법을 다룬다. [10]은 OFDMA와 같은 네트워크의 병렬 채널에서 협력적 간섭 전력을 할당하는 게임 이론적 모델을 제시하였으며, 우호적인 방해자가 다중 채널 도청을 방지하기 위한 전력을 할당하도록 한다. 이와 같이 제안된 대부분의 기존 연구는 모두 하향링크만을 다루고 있으며, 802.11ax 표준에서 처음으로 OFDMA 방식이 상향링크로 채택된 이후에도 여전히 상향링크가 다루어지지 않고 있어 이에 대한 연구가 필요한 실정이다.

3. 시스템 모델

본 장에서는 연구에서 가정하고 있는 공격모델과 제안된 시스템 모델을 설명한다.

3.1 공격 모델

본 연구에서 가정하는 공격모델은 Fig. 2와 같다. 각 공격모델은 STA 2대, AP, 그리고 도청자로 구성된다. STA은 기밀한 정보를 전송하는 사용자인 SU(Secure User)와 일반 정보를 전송하며 간섭을 발생시키는 AU(Assist User)로 구성되어 동시에 AP에게 상향링크 전송을 수행한다. 공격자는 잠재적인 수동적 도청자로, AP에게 숨은 노드인 상태에서 SU의 상향링크 신호를 도청한다. 이때 AP와 STA 간 거리에 따라 공격 모델을 다음과 같이 분류한다. Case 1의 경우 AP와 AU, SU간 거리가 동일하며 Case 2는 SU가 AU보다 AP에게 더 가까이 위치하고, 마지막으로 Case 3은 AU가 SU보다 AP에게 더 가까이 위치하는 경우이다.

$$\text{Case 1: } \text{distance}(AP-AU) = \text{distance}(AP-SU)$$

$$\text{Case 2: } \text{distance}(AP-AU) > \text{distance}(AP-SU)$$

$$\text{Case 3: } \text{distance}(AP-AU) < \text{distance}(AP-SU)$$

3.2 제안 시스템 모델

본 연구에서 20 MHz 대역폭에서의 26-tone 서브채널 배치

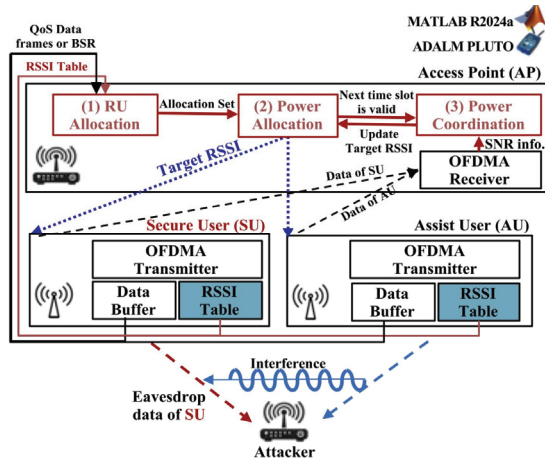


Fig. 3. Procedure of the proposed system block diagram

를 기준으로 최대 사용자는 9명이 될 수 있으나, 다중 사용자 간섭 표현의 간소화를 위해 사용자를 2명으로 가정한다. SU는 AP와의 결합 단계에서 기밀통신 요청을 이미 완료하였다고 가정하며 각 STA들은 상향링크 전송을 수행하기 위한 결합 단계를 이미 수행하였기 때문에 채널 접근 경쟁 (UORA)은 고려하지 않는다.

Fig. 3은 제안된 시스템 블록 다이어그램을 나타낸다. OFDMA 수신기 블록은 AP의 수신부를 나타내며, OFDMA 송신기 블록은 데이터 전송을 수행하는 STA의 송신부를 나타낸다. SU와 AU는 상향링크 전송을 수행하고자 하는 사용자로, AU는 SU의 인접한 서브채널에 배치되어 SU 채널의 보안성을 향상시키도록 도와주는 역할을 수행한다. 먼저 SU에 지리적으로 가장 가깝게 위치한 STA를 AU로 배치하는 것이 보다 적은 전력차로 다중 사용자 간섭을 발생시킬 수 있기 때문에, RU 할당(RU Allocation) 모듈은 SU에게 가장 가까운 STA를 식별한다. 이를 위해 각 STA들은 자신의 주변 STA들로부터 수신된 프로브 요청 프레임의 RSSI(Received Signal Strength Indicator)를 테이블에 주기적으로 업데이트하고, 업데이트된 테이블을 결합 단계 시 AP에게 전달한다. 이후 전력할당(Power Allocation) 및 전력조정(Power Coordination) 모듈은 RSSI 테이블과 기밀통신 요청 정보를 토대로 송신전력 할당을 수행하여 할당된 정보를 각 STA들에게 트리거 프레임으로 전달하고, 다음 타임 슬롯이 유효하는 동안 지속적으로 수신 SNR값을 검증하여 송신전력을 조정한다. 상세한 자원단위 스케줄링, 송신전력 할당 및 조정 모듈의 설명은 4장에서 다룬다.

4. OFDMA 기반 상향링크 통신의 보안성 향상을 위한 전력 조정 스킴

본 장에서는 상향링크 도청 공격모델에서 보안 채널의 보안성을 향상시키기 위해 자원단위의 전력을 할당하고 조정하는 Three-step 스킴을 제안한다.

Algorithm 1: STA selection and RU allocation at AP

```

Initialize:  $T_{SU} = [SSID_x, RSSI_x]$ 
Set: AllIndex={1,...,9},  $\Psi=\{2,4,6,8\}$ 
1: while Resource unit scheduling do
2:    $T_{SU,associated} = AssociateFilter(T_{SU})$ 
3:    $T_{SU,sorted} = SortDescend(T_{SU,associated})$ 
4:    $SSID_{AU} = T_{SU,sorted}[0]$ 
5:   if STA selected:
6:      $SUIndex = AllocationSU(\Psi)$ 
7:      $AUIndex = AllocationAU(\Psi)$ 
8:      $AllocationSet = PF(SUIndex, AUIndex)$ 
9:   end if
10: end while
11: return AllocationSet

```

4.1 자원단위 할당

자원단위 및 전력 할당 모듈은 먼저 SU와 지리적으로 가장 가까운 STA이 주파수 도메인에서 SU의 자원단위에 인접하도록 스케줄링 한다. Algorithm 1은 자원단위 할당을 위한 알고리즘으로 1) STA selection, 2) RU allocation 단계로 구성된다. 먼저 각 STA은 주변 STA들로부터 전송되는 프로브 요청 프레임의 신호 세기를 바탕으로 RSSI 테이블을 주기적으로 업데이트 한다. AP는 결합 단계에서 AssociateFilter를 수행하여 SU가 전달한 테이블에서 결합하고자 하는 STA들을 식별한 후, 식별된 STA들 중 SU와 거리가 가장 가까운 STA를 $SSID_{AU}$ 으로 선정한다. 다음 단계로 AP는 각 트리거 프레임 사이클마다 SU가 배치될 수 있는 RU 인덱스 집합 Ψ 을 {2,4,6,8}으로 할당한다. 해당 인덱스는 가드 부반송파, DC 부반송파로 인한 다중 사용자 간섭의 감소 영향을 최소화 할 수 있는 RU 인덱스로, 각 사이클마다 Ψ 내의 인덱스 중 하나를 선택하여 SU를 할당한다. SU가 할당되면 $SSID_{AU}$ 의 RU를 SU의 RU에 인접하도록 할당한다. 마지막으로 SU, AU를 제외한 STA들은 나머지 RU에 proportional fair 알고리즘을 이용하여 배치된다.

4.2 자원단위 송신전력 할당

송신전력 할당 문제의 결정변수 범위를 초기화하기 위해 먼저 다중 사용자 간섭 영향을 이론적, 실험적 결과와 비교 분석한다. 또한 보안성을 높일 수 있는 다중 사용자 간섭을 최대화하도록 송신전력을 최적화하는 문제를 정의하고, 비밀률 최대화 문제에 비해 계산 복잡도가 낮은 휴리스틱 방식을 사용한 최적화 알고리즘을 제안한다.

1) 다중 사용자 간섭에 따른 SNR 및 EVM 영향 분석

Fig. 4a는 수식 (1)을 기반으로 계산한 총 다중 사용자 간섭 전력을 나타낸 그래프이다. 가정된 잔여 CFO 범위가 350~1500 Hz 이고, 전력차 범위가 0~10 dB일 때의 총 다중 사용자 간섭 전력은 다음과 같다. 이론적으로 계산된 간섭 전력은 잔여 CFO가 커질수록, 전력차가 증가할수록 더 크게 증가함을 보인다. 다음 수식은 전력 차 및 CFO의 함수로서 다중 사

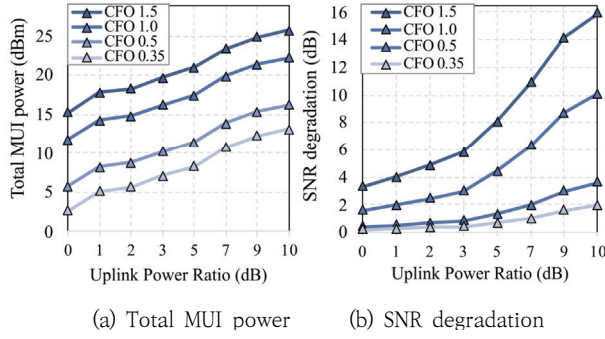


Fig. 4. Impact of MUI per power ratio

용자 간섭에 따른 SNR 저하를 표현한 수식으로, 다중 사용자 간섭으로 인해 발생한 SU의 SNR 저하를 다음과 같이 표현할 수 있다[11].

$$D_{SU} = 10 \cdot \log \left(1 + \frac{M_{i+1}}{N_i} \frac{E_{i+1}}{N_0} \right) \quad (3)$$

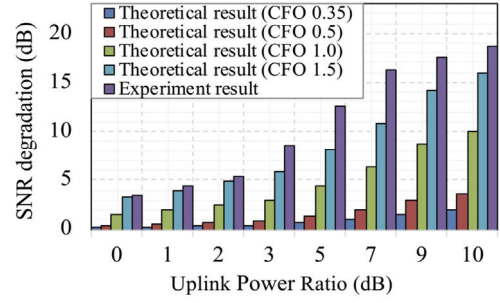
N_i 은 RU_i 의 총 부반송파 개수, M_{i+1} 은 SU에 영향을 받은 총 다중 사용자 간섭 전력, E_{i+1}/N_0 은 송신전력 전력 차 0 dB에서 SU의 SNR이다.

Fig. 4b는 위 수식을 이용하여 SNR 저하를 나타낸 그래프이다. 두 자원단위 간의 송신전력 차이가 10 dB일 때 CFO 0.5 이내의 경우 4 dB 이하의 저하를 보이지만, CFO 1의 경우 10 dB, CFO 1.5의 경우 16 dB, 즉 2.5배 및 4배 가량 저하됨을 확인할 수 있다.

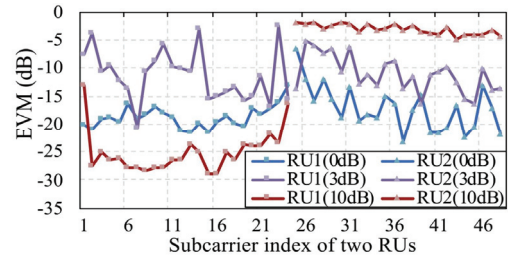
본 연구에서는 다중 사용자 간섭 영향을 이론적으로 분석한 결과와 실험적으로 측정된 결과를 비교하여 분석하기 위해 802.11ax UL-OFDMA 송수신부를 MATLAB에서 구현하였으며, 802.11ax 환경에서의 실제 다중 사용자 간섭 영향을 실험하였다. 실험 환경은 2.4 GHz 대역에서 20 MHz 대역폭에 2개의 서브채널 RU_1 과 RU_2 를 배치하고, 각 서브채널을 AU STA와 SU STA에게 할당한다. 각 STA와 AP간의 거리는 1 m로 동일하게 배치하였으며 MCS는 2, Tx gain과 Rx gain은 각각 0, 10으로 설정하였다. STA의 송신전력 범위는 -3~7 dBm으로, 해당하는 전력 차 범위는 0~10 dB이다.

Fig. 5는 각 사용자의 SNR 및 부반송파 별 EVM을 측정하여 SU의 서브채널에 미치는 다중 사용자 간섭 영향을 보여준다. Fig. 5a는 CFO 및 전력차에 따른 SNR 저하 비교 실험 결과를 나타낸 그래프이다. 실험 결과 전력차가 5 dB 이상일 경우 이론적인 분석 결과와 달리 SNR 저하가 현저하게 증가하였으며, BPSK를 기준으로 5 dB를 초과하는 전력차가 발생할 경우 SNR이 약 17 dB 저하되어 비트 에러율(bit error rate, BER)은 50%에 도달한다.

Fig. 5b는 서브채널 내 개별 부반송파에서 다중 사용자 간섭 영향을 확인하기 위해 부반송파 별 EVM을 나타낸다. 해당



(a) Comparison of SNR degradation



(b) EVM per each subcarrier between two RUs

Fig. 5. SNR degradation and EVM distribution by power ratio

그래프는 전력차를 0~10 dB 범위로 조정하며 각 서브채널 내 부반송파 인덱스별 EVM을 나타내는 그래프이다. 실험 결과 두 서브채널 간 가장 가깝게 위치하는 부반송파 인덱스의 EVM은 가장 큰 간섭 영향을 겪기 때문에 EVM이 더 크게 저하됨을 보인다. 실험 결과 두 서브채널 간의 평균 EVM은 전력차가 3 dB 이하일 경우 2 dB 이내, 10 dB 경우 20 dB 이상 차이가 발생한다.

2) 송신전력 할당 문제

본 연구는 무선랜 기기의 제한된 계산 능력 및 실시간 처리 요구사항을 고려하여, 송신전력 최적화 문제를 무선랜 기기가 처리하기에 적합한 문제로 정의한다. 일반적으로 비밀률의 최대화 문제는 로그 함수의 차이로 정의되기 때문에 non-convex 문제이며, 이는 높은 계산 복잡성을 가지고 많은 계산 자원을 필요로 한다[1]. 따라서 본 연구는 간접적으로 보안성을 높일 수 있는 다중 사용자 간섭을 최소화 하도록 송신전력을 최적화 하는 문제를 정의한다. 제안된 알고리즘은 비밀률 최대화 문제에 비해 비교적 단순하고 제약조건을 명확히 정의하여 휴리스틱 방식인 담금질 알고리즘으로 최적화를 수행한다. 아래 수식은 두 서브채널의 송신전력을 초기 할당하기 위한 문제이다.

$$\begin{aligned} & \max_{p_i, p_{i+1}} M_{i+1}; \\ & \text{s.t. } SINR_i < SINR_{i+1}; \quad i \in S, \\ & \quad SINR_i > SINR_{MCS_i}^{Threshold} \quad MCS = 1, \dots, 4 \end{aligned} \quad (4)$$

위 문제는 SU의 채널을 저하시키기 위해 제약조건을 만족

Algorithm 2: Power allocation with SU and AU

Initialize: initial temperature $T_i=100$, final temperature $T_f=1$, coolingrate $R=0.9$, max iteration $j=1000$, power lower $L=-3$, power upper $U=7$, frequency offset $f=0.5$
Set: best objective S_B , candidate objective S_C , required minimum SNR δ , noise power of SU w_{SU} , noise power of AU w_{AU}
Let: current temperature $T = T_i$, $\phi = rssi_{AU} - rssi_{SU}$
Define: $constraint(\delta, S_C, p_{SUcandidate}, p_{AUcandidate})$
 $SINR_{SU} = 10 \log_{10}(p_{SUcandidate} / (S_C + w_{SU}))$
 $SINR_{AU} = 10 \log_{10}(p_{SUcandidate} / (objectiveMUI(p_{AUcandidate}, p_{SUcandidate}) + w_{AU}))$
 $constraint = SINR_{SU} < SINR_{AU} \wedge SINR_{SU} > \delta$
 return $constraint \rightarrow$ True or False

```

1: if  $-1 \leq \phi \leq 1$ : → CASE 1
2:    $p_{SU}, p_{AU} = L$ 
3: else if  $\phi < -1$ : → CASE 2
4:    $p_{AU} = rand(L + 3dB, U)$ 
5: else → CASE 3
6:    $p_{SU}, p_{AU} = L$ 
7:   return  $p_{SU}, p_{AU}$ 
8: end if
9: while  $T > T_f$  do
10:  for  $i$  in  $1:j$  → take a step
11:     $p_{SUcandidate} = p_{SU} + rand() - 0.5 * 2 * T / T_i$ 
12:     $p_{AUcandidate} = p_{AU} + rand() - 0.5 * 2 * T / T_i$ 
13:     $S_C = objectiveMUI(p_{SUcandidate}, p_{AUcandidate})$ 
14:    → evaluate candidate point
15:     $T = T * R$ 
16:    if  $constraint(\delta, S_C, p_{SUcandidate}, p_{AUcandidate})$  is True:
17:      if  $S_C > S_B \vee rand() < \exp((S_C - S_B) / T)$ :
18:         $p_{SU}, p_{AU} = p_{SUcandidate}, p_{AUcandidate}$ 
19:         $S_B = S_C$  → update best objective value
20:      end if
21:    end if
22:  end for
23: end while
24: return  $p_{SU}, p_{AU}$ 

```

하면서 목적함수인 다중 사용자 간섭을 최소화할 수 있는 AU와 SU의 초기 송신전력을 찾는 문제이다. 제약조건은 총 다중 사용자 간섭 영향을 받은 SU의 SINR이 AU의 SINR보다 낮아야 하고, 동시에 SU의 데이터를 디코딩할 수 있는 최소 SNR 보다는 높아야 한다. AP는 송신전력 초기 할당 시 수식 (2)와 프로브 요청 프레임 신호 상태를 이용하여 각 서브채널의 SINR을 계산할 수 있으며, 낮은 SINR으로 디코딩을 수행해야 하기 때문에 MCS의 범위를 {0,1,2,3,4}으로 할당한다. $p_i, p_{i \pm 1}$ 의 범위는 10 dB 전력비를 가질 수 있도록 $-3 \sim 7$ dBm으로 초기화한다.

제안된 자원단위 송신전력 할당 모듈은 SU에 다중사용자 간섭 영향을 적절히 미칠 수 있도록 송신전력 할당 문제를 푸는 역할을 수행한다. 전력차를 0 dB부터 점차 증가시켜 AP가 SU 데이터를 디코딩할 수 있도록 SU의 채널 상태를 MCS의

Algorithm 3: Iterative power coordination

Initialize: iteration index $r=1$, scale factor $s=1.1$
Set: $\delta, p'_{SU}, p'_{AU}, SINR'_{SU}, SINR'_{AU}$

```

1: while Power coordination do → next time slot is valid
2:   if  $SINR'_{SU} < \delta$  at AP:
3:      $p'^{r+1}_{SU} = p'_{SU} * s$ 
4:   else if  $SINR'_{AU} < \delta$  at AP:
5:      $p'^{r+1}_{AU} = p'_{AU} * s$ 
6:   else:
7:     break → exiting the loop of power coordination
8:   end if
9: end while

```

최소 요구 SNR에 근접하도록 저하시킨다. 서브채널 간 전력 차 할당은 AU 채널의 SNR이 SU 채널의 SNR보다 높도록 하면서, 동시에 SU의 채널이 최소 SNR을 달성할 수 있는 송신 전력으로 할당한다. Algorithm 2는 세 가지로 분류된 공격모델 조건에서 제약조건을 만족하는 초기 송신전력을 최적화한다. Case 1의 경우 SU, AU의 초기 송신전력 하한 값을 동일하게 -3 dBm으로 초기화하고, Case 2의 초기전력은 RSSI(dBm) 차이에 따라 할당된다. RSSI 차가 -1 보다 작으면 AU의 초기 전력은 SU보다 3 dB 높도록 초기화된다. Case 2의 경우 SU가 보다 더 강한 수신신호를 가지기 때문에 도청자에게 유리하지 않은 상황이다. 그러나 0 dB로 초기화될 경우 거리가 크게 차이나지 않는다면 채널상태 저하를 겪음에도 불구하고 여전히 디코딩될 수 있다. 따라서 AU의 전력 하한값을 3 dB 차이 나도록 초기화한다. Case 3의 경우 SU가 도청자에게 더 가까운 거리이기 때문에, BER 저하가 상대적으로 미미하더라도 AP의 디코딩이 가능하도록 전력비 0 dB를 할당한다. 담금질 알고리즘의 반복 수는 전역 최적해에 가까울 수 있도록 1,000회로 설정하고, 각 반복마다 초기 온도에서 종료 온도로 냉각하여 검색한다. R 은 냉각 속도를 의미하며 초기 온도에서 종료 온도로 서서히 냉각하는 과정에서 온도를 감소시키는 비율을 나타낸다.

S_B 는 검색 과정에서 목적함수의 최댓값을 유지하며 S_C 는 각 반복 시 목적함수의 후보 값을 저장한다. 새로운 솔루션 수용 여부는 후보 솔루션이 현재의 최적 솔루션보다 우수할 경우에 이를 수용하지만, 후보 솔루션이 더 나쁜경우에도 목적함수 평가의 차이를 바탕으로 계산된 확률에 따라 수용될 수도 있다. 수용 확률은 현재 온도 T 에 의존하기 때문에 검색 초기에서 지역 최솟값에서 벗어날 수 있도록 하여 검색 후반이 될수록 최적값을 연마할 수 있다.

$objectiveMUI$ 함수는 수식 (1)의 함수로서 후보 솔루션의 목적함수 값을 평가하며, 각 검색 반복 시 초기화 되는 $p_{SUcandidate}, p_{AUcandidate}$ 을 입력으로 후보 솔루션을 계산한다. $constraint$ 함수는 MCS의 최소 요구 SNR δ , 현재 후보 솔루션으로 평가한 목적함수 값 S_C , 그리고 $p_{SUcandidate}, p_{AUcandidate}$ 솔루션을 입력으로 제약조건을 만족를 검증한다. 본 연구에서

제안하는 알고리즘은 SINR 및 최소 요구 SNR 조건들을 충족시키는 것이 성능을 보장하는 데 필수적이기 때문에, 각 반복마다 제약 조건을 검증하는 방식을 적용한다.

4.3 자원단위 송신전력 조정

자원단위 송신전력 조정 모듈은 i -th 상향링크 시간 슬롯에서의 SU, AU의 자원단위 송신 전력을 조정한다. Algorithm 3은 직전 타임슬롯에서 SU, AU로부터 수신한 상향링크 채널 상태를 이용하여 최소 요구 SNR 값 만족 여부를 검증하고, 이에 미달 시 다음 반복 인덱스를 증가시켜 p_{SU}^{i+1} , p_{AU}^{i+1} 의 송신전력을 증가시킨다. 다음 타임슬롯이 유효하는 동안 해당 검증을 반복 수행한다.

5. 성능 평가

본 장에서는 제안된 기법의 성능 평가를 위해 실험 결과를 상세히 분석한다.

5.1 실험 환경

본 연구에서는 ADALM-PLUTO와 MATLAB R2024 WLAN Toolbox를 사용하여 제안된 기법을 구현하였다. 주파수 대역은 2.4 GHz로 설정하였으며, 20 MHz 채널 대역폭에서 26-tone의 두 서브채널을 각 STA에 할당하였다. 실험을 위해 총 2대의 STA와 1대의 AP, 1대의 도청자를 구성하였다. MCS는 낮은 SNR에서 디코딩을 수행해야 하기 때문에 0부터 4까지 낮은 범위로 가정하여 실험한다.

ADALM-PLUTO의 최대 전송 전력은 7 dBm 이므로 10 dB 전력비를 가질 수 있는 p_i , p_{i+1} 의 범위는 $-3 \sim 7$ dBm 으로 초기화한다. 본 실험의 평가 매트릭은 BER과 비밀률(secretacy rate)으로, 비밀률은 비밀 통신이 가능한 사용자의 데이터 전송률과 도청자의 데이터 전송률 사이의 관계를 표현하고, 다음과 같이 표현한다[3].

$$r^s = [r_{AP} - r_{eve}]^+ \quad (5)$$

$$r^s = \log(1 + SNR_{AP}) - \log(1 + SNR_{eve})$$

r^s 는 주어진 채널에서 초당 전송되는 최대 비밀 비트 수를 의미하며, r_{AP} 와 r_{eve} 는 각각 합법적인 채널과 도청 채널에서의 최대 데이터 전송률을 의미한다. 비밀률은 0보다 작을 경우 0, 양수일 경우 그 값을 그대로 사용한다. 즉, $[x]^+ = \max(0, x)$ 이다.

본 실험의 성능 평가는 하나의 패킷 당 최대 비트를 전송하였을 때의 비트에러율과 비밀률을 측정하여 보안성 향상을 평가하였으며, SNR과 BER에 대해 5회 반복 실험을 수행하여 오류로 인한 실험 오차를 최소화 하였다.

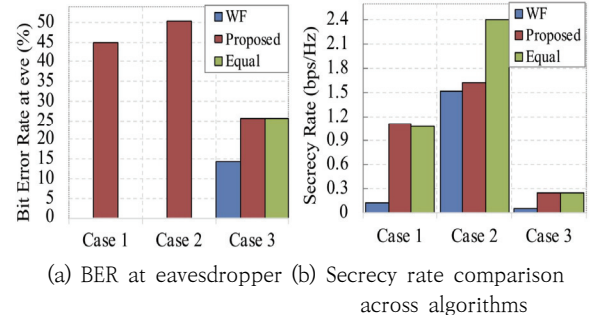


Fig. 6. Comparison of BER and secrecy rate for well-known algorithm

Table 1. Distance in each case

	SU-AP	AU-AP	SU-Eve	AU-Eve
Case 1	1 m	1 m	1.5 m	1.5 m
Case 2	0.5 m	1 m	2 m	1.5 m
Case 3	1 m	0.5 m	1.5 m	2 m

5.2 실험 결과

Fig. 6은 자원단위 전력 스케줄링 알고리즘으로 잘 알려져 있는 균등 전력 할당, water-filling 알고리즘과 제안된 알고리즘을 비교하여 잠재적인 도청자의 BER 및 향상된 비밀률을 보여준다. 제안된 알고리즘의 경우, 모든 Case에 대해 기존 알고리즘보다 도청자의 높은 BER과 향상된 비밀률을 보인다. 이때 MCS는 0으로 설정되었으며, Case 별 설정한 각 주체 간 거리는 Table 1과 같다.

Fig. 6a는 각 알고리즘에서의 Case 별 BER을 측정하여 잠재적 도청자가 SU의 상향링크 신호를 정상적으로 디코딩 할 수 없음을 보여준다. 본 연구에서 전력 할당 및 조정 절차를 거쳐 최종 할당된 전력차는 Case 별로 5.3 dB, 3.1 dB 그리고 0 dB이다. Case 1의 경우 최대 MUI를 발생할 수 있도록 큰 전력비가 할당되고, Case 2는 SU의 거리가 더 근접하기 때문에 적은 전력비로도 높은 BER을 달성할 수 있으며, Case 3의 경우 멀리 위치한 SU의 SNR이 최소 요구 SNR 값 이상이 되도록 적은 전력비가 할당된다. 5회 반복 실험 결과 도청자가 수신한 SU 신호의 평균 BER은 45%, 50.2%, 25.6%에 도달하여 기존의 알고리즘보다 디코딩 실패가 현저하게 증가함을 확인할 수 있으며, 이 때 AU의 BER은 모두 0%이다. 자원단위에 동일한 전력을 할당하거나, 채널 상태가 더 높은 자원단위에 더 높은 전력을 할당할 경우 BER은 Case 1, 2의 경우 0으로 잠재적인 도청자가 모든 기밀한 정보를 디코딩할 수 있으며, Case 3의 경우 최대 25.6%에 도달한다. Case 2의 경우 SU와 잠재적인 도청자 간의 채널 상태가 다른 Case보다 낮기 때문에 상대적으로 낮은 전력차로도 보안성 향상에 효과적임을 확인할 수 있다.

Fig. 6b는 합법적인 채널과 도청 채널에서의 비밀률을 비교한 그래프이다. 해당 실험 결과는 합법적인 채널과 도청 채널에서 측정된 SNR을 토대로 비밀률이 계산되었다. 제안된 기

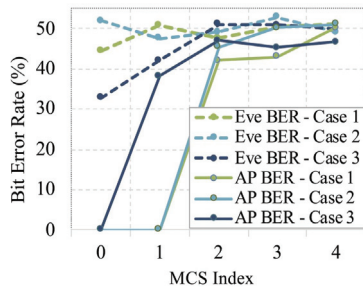
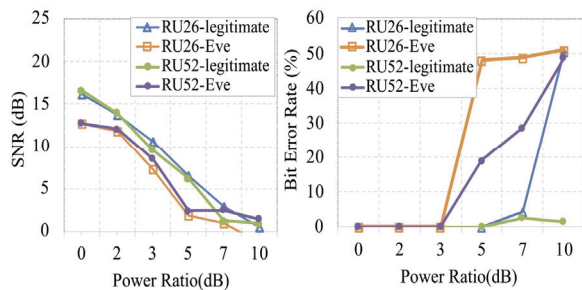


Fig. 7. BER performance for eve and AP in different cases with varying MCS



(a) SNR at each channel (b) BER at each channel

Fig. 8. Comparison of SNR and BER for two RU sizes for legitimate and eavesdropping channels

법은 정당한 채널을 요구된 최소 SNR 값에 근접하게 저하시키기 때문에, 비밀률이 아닌 실제 측정된 BER로 합법 채널의 보안성을 평가한다. 해당 그래프는 Fig. 6a 실험 결과에 해당하는 채널의 보안율을 나타내며, 제안된 스킴을 적용할 경우 각각 1.12 bps/Hz, 1.62 bps/Hz, 0.24 bps/Hz를 달성한다. 해당 실험 결과 다른 알고리즘들과 비교하여 비슷하거나 낮은 비밀률이 측정되나, 실제 통신 환경에서 측정된 BER은 모든 Case에 대해 높으므로 보안이 향상됨을 확인할 수 있다.

Fig. 7은 MCS 인덱스별로 달라지는 BER의 영향을 시각화한 그래프로, 모든 Case에서의 각 AP, 도청 채널에 SU 신호의 BER을 비교한다. 해당 실험 결과를 토대로 Case 1,2의 경우 도청자로부터 안전하게 신호를 전송하기 위해 최대 MCS 1까지 통신 할 수 있으며, Case 3의 경우 MCS 0으로 통신함으로써 목적함수를 달성할 수 있음을 확인하였다.

Fig. 8은 Case 1에서 RU 크기를 26-tone, 52-tone 별로 실험하여 자원단위의 크기에 따른 MUI 영향을 확인하기 위한 그래프이다. 52-tone은 26-tone에 비해 두 배의 대역폭 크기를 가지기 때문에 다중 사용자 간섭의 민감도가 상대적으로 낮아지므로 실험 결과 각 52-tone에서의 SNR은 26-tone보다 2 dB가량 높게 측정되었으며, BER은 전력차가 5 dB일 경우 약 29%, 7 dB일 경우 약 20% 낮아짐을 확인할 수 있다. 따라서 실제 사용 환경에서 보다 적은 전력차로 다중 사용자 간섭을 발생시킬 수 있도록 하는 26-tone을 사용하는 것이 효율적임을 확인할 수 있다.

6. 결 론

본 논문에서는 OFDMA 상향링크에서의 보안성 향상을 목적으로 한 전력 할당을 최초로 논의하며, 다중 사용자 간섭을 의도적으로 유도하여 보안을 강화하는 전력 할당 및 조정 기법을 제안하였다. 특히, 다중 사용자 간섭의 영향을 실험적으로 분석한 결과를 토대로 설계된 제안 기법은 IEEE 802.11ax 표준을 만족하도록 고려되어 실질적인 의의를 가진다. 연구진은 다중 사용자 간섭의 영향을 분석하기 위해 전력비에 따른 SNR 및 EVM의 변화를 실험적으로 평가하였으며, 제안된 기법과 일반적인 전력 할당 알고리즘 간의 BER 및 비밀률을 비교한 결과, 추가적인 간섭 주체 없이 자체적으로 채널의 보안성을 향상시킬 수 있음을 확인하였다. 제안된 기법을 적용한 전력 할당 및 조정을 통해 기밀 데이터를 전송한 결과, 모든 공격 모델에서 합법적인 AP의 비트 오류율이 0%를 기록한 반면, 도청자의 비트 오류율은 각각 45%, 50.2%, 25.6%에 도달하여 제안된 기법이 보안성을 크게 향상시킴을 입증하였다.

제안된 기법은 성능 비용 관점에서 STA 별 전력 차이를 균등하게 하여 통신 성능을 향상시키는 목표와 상충되어 비용이 발생할 수 있다. 그러나 보안성 확보는 대부분의 경우 채널용량 및 처리량 감소의 비용을 수반하며, 금융정보 또는 개인정보를 포함하는 기밀한 서비스를 사용하는 사용자는 이러한 추가 비용을 기꺼이 감수할 가능성이 높다[2]. 따라서 향후 연구에서는 채널용량 감소의 비용을 최소화하면서 보안성을 높일 수 있는 시스템을 제안할 계획이며, 실제 네트워크 환경에서의 적용 가능성을 높이기 위해 최대 다중 사용자 수 및 다양한 자원 단위 구성을 고려한 배포 전략 및 효율적인 시스템 설계를 후속 연구에서 제안할 계획이다.

References

- [1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, Vol.21, No.2, pp.1773-1828, 2019.
- [2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proc. of the IEEE*, Vol.104, No.9, pp.1727-1765, 2016.
- [3] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," in *Proc. of IEEE International Symposium on Information Theory*, pp.356-360, 2006.
- [4] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A Tutorial on IEEE 802.11ax High Efficiency WLANs," *IEEE Communications Surveys & Tutorials*, Vol.21, No.1, pp.197-216, 2019.

- [5] A. Wang, J. Chen, Y. Cai, C. Cai, W. Yang, and Y. Cheng, "Joint subcarrier and power allocation for physical layer security in cooperative OFDMA networks," *EURASIP Journal on Wireless Communications and Networking*, Vol.2013, No.193, pp.1-13, 2013.
- [6] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Proc. of International Conference on Telecommunications*, 2008.
- [7] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks," *IEEE Transactions on Information Forensics and Security*, Vol.6, No.3, pp.693-702, 2011.
- [8] S. Karachontzitis, S. Timotheou, I. Krikidis, and K. Berberidis, "Security-Aware Max-Min Resource Allocation in Multiuser OFDMA Downlink," *IEEE Transactions on Information Forensics and Security*, Vol.10, No.3, pp.529-542, 2015.
- [9] Y. Sun, D. Wing K. Ng, and R. Schober, "Resource allocation for secure full-duplex OFDMA radio systems," in *Proc. of IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications*, 2017.
- [10] Z. Xu and M. Baykal-Gürsoy, "Power Allocation for Cooperative Jamming Against a Strategic Eavesdropper Over Parallel Channels," *IEEE Transactions on Information Forensics and Security*, Vol.18, pp.846-858, 2023.
- [11] L. Wilhelmsson and N. Butt, "Analysis of frequency and power requirements for UL-OFDMA," *IEEE 802.11-14/1446r0*, Nov. 2014.



박 현 주

<https://orcid.org/0000-0002-7181-0911>
 e-mail : hjpark01@korea.ac.kr
 2021년 성신여자대학교 융합보안공학과(학사)
 2021년~현 재 고려대학교
 정보보호대학원 석사과정

관심분야 : IoT 보안, 네트워크 보안, RF 기반 보안 기술



이 원 준

<https://orcid.org/0000-0001-5286-6541>
 e-mail : wlee@korea.ac.kr
 1989년 서울대학교 컴퓨터공학(학사)
 1991년 서울대학교 컴퓨터공학(석사)
 1999년 University of Minnesota,
 Minneapolis 컴퓨터공학(박사)

2002년~현 재 고려대학교 정보보호대학원 교수

관심분야 : 무선 저전력 통신, 차세대 유무선 네트워크 프로토콜, 모바일 네트워킹/컴퓨팅, 무선 보안, 네트워크 최적화