https://doi.org/10.7840/kics.2025.50.8.1172

위장 공격에 대한 합성곱 신경망 기반의 물리계층 인증

오 한 올◆, 윤 지 현*, 문 지 환**, 김 태 훈**, 방 인 규°

CNN-Based Physical Layer Authentication against Impersonation Attacks

Hanol Oh◆, Jihyeon Yoon*, Jihwan Moon**, Taehoon Kim**, Inkyu Bang°

요 약

본 연구에서는 디지털 식별자 기반의 기존 WLAN (wireless local area network) 보안 프로토콜이 가지는 위장 공격(impersonation attack)에 대한 취약점을 개선하기 위해 합성곱 신경망(convolutional neural network) 기반 물리계층 인증(physical layer authentication, PLA) 기법을 제안하고 실험을 통해 공격 탐지 정확도를 평가한다. 본 연구의 주요 결과는 다음과 같다. 첫째, 위장 공격의 한 종류인 이블 트윈(evil twin) 공격을 구현하고 기존 WLAN 보안 프로토콜의 취약점을 확인한다. 둘째, 기기(device)의 이동성이 없는 정적 무선 환경에서는 채널 상태 정보(channel state information, CSI)를 활용한 PLA 기법이 높은 공격 탐지 정확도(99.3%)를 보이지만 기기의 이동성이 존재하는 동적 무선 환경에서는 낮은 공격 탐지 정확도(35.0%)를 보이는 것을 실험을 통해 확인한다. 셋째, CSI을 활용한 PLA 기법의 한계점을 극복하기 위해 기기의 고유특성인 IQ 불균형(IQ imbalance)을 활용한 합성곱 신경망 기반 PLA 기법을 제안하고 모의실험을 통해 공격 탐지 정확도를 평가한다.

키워드 : 물리계층 인증, 합성곱 신경망, 위장공격, 채널 상태 정보, IQ 불균형

Key Words : Physical Layer Authentication (PLA), Convolutional Neural Network (CNN), Impersonation Attack, Channel State Information (CSI), IQ Imbalance

ABSTRACT

In this paper, we propose a convolutional neural network (CNN)-based physical layer authentication (PLA) scheme as a countermeasure against impersonation attacks in WLAN (Wireless Local Area Network). We evaluate the proposed PLA scheme in terms of attack detection rate through experiments. The main contributions are as follows: (1) We implement the Evil Twin attack which is one of the impersonation attacks in WLAN; (2) We implement the channel state information (CSI)-based PLA scheme and perform experiments to measure attack detection rates in both static and dynamic channel environments; (3) We finally propose the CNN-based PLA scheme exploiting the unique IQ imbalance of hardware and evaluate its performance through extensive simulations.

※ 이 논문은 2024년도 교육부 및 한국연구재단의 국립한밭대학교 국립대학육성사업으로 지원된 연구임.
※ 이 논문의 일부는 한국통신학회 2024년도 하계종합학술발표회('24.06.19~'24.06.22)에서 발표되었습니다.
◆ First Author : Hanbat National University, Department of Intelligence Media Engineering, ohhanol5957@gmail.com, 학생회원
° Corresponding Author : Hanbat National University, Department of Intelligence Media Engineering, ikbang@hanbat.ac.kr, 종신회원
* 세림티에스지(주)
** Hanbat National University
논문번호 : 202502-029-C-RU, Received January 30, 2025; Revised March 1, 2025; Accepted March 18, 2025

Ⅰ. 서 론

이동통신 시스템의 진화 및 발전과 함께 IEEE 802.11로 대표되는 무선 근거리 통신망(Wireless Local Area Network, WLAN) 기술 역시 급속한 발전과 확산을 이뤄왔다. 무선통신 기술의 발전으로 차세대 모빌리티 등을 포함한 다양한 응용 애플리케이션의 등장이 기대되고 있는 상황이다[1].

특히, 드론은 빠르고 유연한 이동성을 기반으로 다양한 분야에서 효율성을 극대화하며 그 활용 범위가 지속적으로 확대되고 있다. 그러나 드론 운용에 주로 사용되는 IEEE 802.11 기반의 통신 프로토콜의 일부는 MAC 주소와 SSID 같은 단순한 디지털 식별자를 기준으로 사용자 기기(device)를 식별하고 있다[2]. 무선통신 시스템에 대한 보안성이 더욱 중요해지고 있는 상황에서 디지털 식별자 기반의 사용자 식별 및 인증 방식은 다양한 무선 보안 취약점을 초래할 수 있다[3].

위장 공격(impersonation attack)은 공격자가 합법적 AP (access point)인 것처럼 위장하여 사용자를 기만하는 공격이다[4]. WLAN에서 구현 가능한 위장 공격의 대표적인 유형으로 이블 트윈(evil twin) 공격이 있으며 그림 1과 같다. 공격자는 합법적 AP와 동일한 SSID 및 MAC 주소를 가지는 가짜 AP를 생성하여 사용자를 위장 공격자가 구성한 네트워크로 연결하도록 유도한다. 위장 공격이 성공할 경우, 네트워크 트래픽이 도청되어 민감한 정보가 탈취되는 등 심각한 보안 문제가 발생할 수 있다[5].

이러한 보안 문제를 극복하기 위해 최근 물리계층 인증(physical layer authentication, PLA) 기법이 주목받고 있다[6]. PLA 기법은 무선 채널 정보 등의 사용자 기기에서만 활용할 수 있는 물리적 특성을 활용하여 송신기의 진위 여부를 검증하는 보안 기법이다. PLA 기법은 디지털 식별자와 달리 상대적으로 위조가 어려운 물리계층 정보를 활용하기 때문에 위장 공격에 대한 대응책으로 활용될 수 있다.

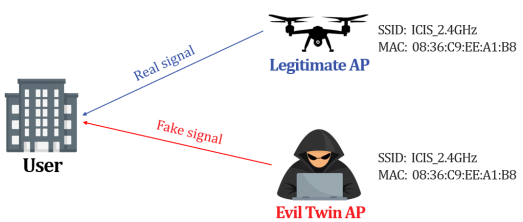

그림 1. Evil Twin 공격에 취약한 기존 WLAN 보안 프로토콜
Fig. 1. Conventional WLAN security protocol vulnerable to Evil Twin attack

이에 PLA 기법을 활용하여 무선 네트워크 보안을 강화하려는 다양한 연구가 최근 제안된 바 있다. 합성곱 신경망(convolutional neural network, CNN) 기반 분류 모델을 통해 이블 트윈 공격을 탐지하는 연구[7,8]와 이동성 있는 환경에서 채널 상태 정보(channel state information, CSI)를 활용하는 물리계층 인증 기법을 제안하는 연구[9,10] 등이 대표적이다. 또한, 무선 채널 정보를 기반으로 안정적인 공격자 탐지가 가능하도록 PLA 기법을 개선하는 연구도 진행된 바 있다. 채널 통계를 고려하지 않고도 송신기 장치를 분류하는 기법[11], 전력 증폭기의 비선형성을 활용하여 시간 변동 채널에서도 장치를 식별하는 기법[12], 다중경로 페이딩 환경에서 채널 변화에 강인한 식별 기법[13], 무선 전송 다이버시티를 적용하여 탐지 성능을 향상시키는 기법[14] 등이 제안된 바 있다. 그러나 선행 연구에서 제안한 PLA 기법은 대부분 정적 환경 또는 특정 채널 환경을 가정하거나, 악의적 사용자의 무선 데이터 수집 등을 가정하므로 실질적 PLA 기법 사용의 제약사항이 될 수 있다. 또한, 일부 연구에서는 채널 변동에 강인한 탐지 기법을 제안하였으나, 기본적으로 채널 환경을 학습하므로 공격자와 합법적 장치가 유사한 채널을 공유하거나 드론과 같이 이동성 높은 환경이라면 탐지 성능이 저하할 수 있다. 따라서 실제 하드웨어 기반의 동적 환경에서 위장 공격의 효과를 체계적으로 분석하고 다양한 무선 환경에 적용 가능한 PLA 기법에 대한 연구가 필요한 상황이다.

이에 본 논문에서는 정적 무선 환경뿐만 아니라 동적 무선 환경에서도 이블 트윈 공격 등의 위장 공격을 효과적으로 탐지할 수 있는 CNN 기반의 물리계층 인증 기법을 제안하고, 공격 탐지 정확도를 평가한다. 본 논문의 주요 결과는 다음과 같다.

① 본 논문에서는 위장 공격의 한 종류인 이블 트윈(evil twin) 공격을 구현하고 기존 WLAN 보안 프로토콜의 취약점을 확인하였다.

② 본 논문에서는 사용자 기기(device)의 이동성이 없는 정적 무선 환경에서는 CSI를 활용한 PLA 기법이 높은 공격 탐지 정확도(99.3%)를 보이지만 기기의 이동성이 존재하는 동적 무선 환경에서는 낮은 공격 탐지 정확도(35.0%)를 보이는 것을 실험을 통해 확인하였다.

③ CSI를 활용한 PLA 기법의 한계점을 극복하기 위해 기기의 고유특성인 IQ 불균형을 활용한 합성곱 신경망 기반 PLA 기법을 제안하고 모의실험을 통해 공격 탐지 정확도를 평가한다.

본 논문은 총 5장으로 구성되어 있으며, 각 장의 내

표 1. 약어 설정
Table 1. Description of abbreviations

Abbreviation	Description
16QAM	16-Quadrature Amplitude Modulation
AP	Access Point
AWGN	Additive White Gaussian Noise
CSI	Channel State Information
CSI-A	CSI-based Authentication
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IQ-A	I/Q imbalance-based Authentication
MAC	Media Access Control
PLA	Physical Layer Authentication
QPSK	Quadrature Phase Shift Keying
SDR	Software Defined Radio
SSID	Service Set Identifier
WLAN	Wireless Local Area Network

용은 다음과 같다. Ⅱ장에서는 본 논문에서 다루는 시스템 모델을 설명하고, Ⅲ장에서는 CSI와 IQ 불균형 정보를 활용하는 CNN 기반 PLA 기법을 설명한다. Ⅳ장에서는 인증 기법의 성능 평가를 위한 실험 환경에 대해 다루며, 실험 결과는 공격 탐지 정확도 관점에서 평가한다. 마지막으로 Ⅴ장에서는 본 논문에서 논의된 내용을 정리하고 결론을 맺는다. 표 1은 본 논문에서 사용되는 약어이다.

Ⅱ. 시스템 모델

본 장에서는 그림 2와 같이 시스템 모델의 전체적인 구성을 소개한다. 구체적으로, 이블 트윈 공격을 포함한 위협 모델과 함께 본 연구에서 활용하는 채널 상태 정보 및 IQ 불균형에 대한 개념을 소개한다.

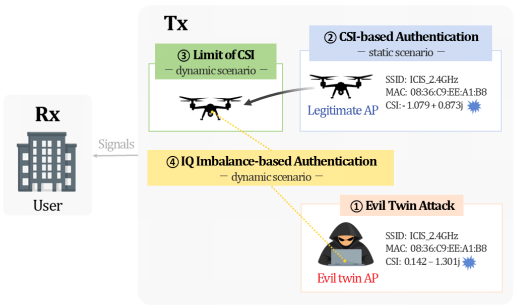

그림 2. 전체 구성
Fig. 2. Overall configuration

2.1 위협 모델

본 연구에서는 수신기 또는 송신기가 움직일 수 있는 이동성이 있는 환경에서 두 단말이 WiFi를 이용하여 무선 통신을 하는 상황을 가정한다. 위협 모델로 위장 공격의 한 종류인 이블 트윈 공격을 가정하며 공격자는 두 단말의 이동 경로를 알고있다고 가정한다. 공격자의 목표는 이블 트윈 공격을 통해 공격자가 설정한 가짜 AP에 사용자 단말이 연결되는 것이며, 본 연구에서 제안하는 CNN 기반 PLA 기법의 최종 목표는 이러한 위장 공격을 탐지하는 것이다.

본 논문에서는 이블 트윈 공격의 구현을 통해 WLAN 보안 프로토콜의 취약성을 실험적으로 검증하였다. 이블 트윈 공격은 공격자가 합법적 AP와 동일한 SSID 및 MAC 주소를 가지는 가짜 AP(즉, 이블 트윈 AP)를 생성하여 사용자가 이를 합법적 AP로 오인하게 만드는 공격 방식이다. 공격자는 사용자를 위장된 네트워크로 유도한 뒤 네트워크 트래픽을 가로채거나 민감한 정보를 탈취할 수 있다.

이블 트윈 AP는 Kali Linux와 Aircrack-ng 도구를 활용하여 생성할 수 있다. 공격 구현 과정은 그림 3과 같다. Airmon-ng를 사용하여 무선랜 인터페이스를 모니터 모드로 설정하고 Airodump-ng를 통해 주변 무선 네트워크를 스캔하여 공격 대상 AP에 대한 데이터를 수집한다. 이후, 수집된 데이터를 기반으로 Airbase-ng를 활용하여 이블 트윈 AP를 생성하며, DNS 및 DHCP

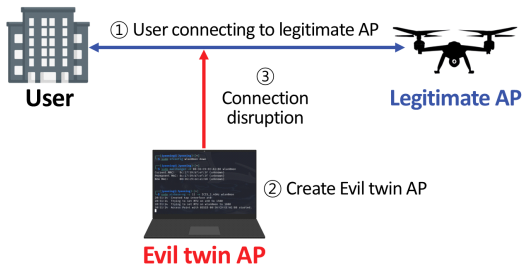

그림 3. 이블 트윈 공격 모델
Fig. 3. Evil twin attack model

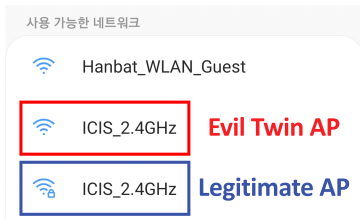

그림 4. Evil twin AP 생성 결과
Fig. 4. Result of creating Evil twin AP

서비스를 설정하여 가짜 AP 기능을 활성화한다. 마지막으로, Airplay-ng를 사용하여 사용자에게 인증해제(deauthentication) 패킷을 전송하고, 사용자와 합법적 AP 간 연결을 강제 해제 및 이블 트윈 AP로의 연결을 유도한다.

그림 4는 이블 트윈 공격의 구현 결과이다. 이블 트윈 AP를 생성하여 합법적 AP와 동일한 AP를 생성하고 연결을 강제할 수 있음을 확인할 수 있다.

2.2 채널 상태 정보(CSI)

CSI는 무선 신호가 공기 중을 통과하며 발생하는 변화를 정량적으로 나타내는 값이다. 신호의 전파 경로, 반사, 회절, 산란 등 물리적 요인에 따라 CSI가 결정되며, 송신기의 위치와 채널 환경에 따라 고유한 특성을 가진다. 이러한 특성은 송신기에서 발생하는 신호의 고유성을 분석하는 데 활용할 수 있어, 정적 무선 환경에서 위장 공격(이블 트윈 공격)을 탐지하는데 유용하게 사용될 수 있다. 그러나 CSI만을 활용하여 송신기를 식별할 경우 위치 및 환경에 따라 민감하게 변화하는 CSI의 특성으로 인해, 동적 무선 환경에서는 안정적인 공격 탐지가 어려울 수 있다. 본 연구에서는 합법적 기기의 CSI를 학습하여 위장 공격을 분류하는 CNN 기반 인증 기법을 CSI 기반 인증(CSI-based authentication 또는 CSI-A) 기법이라고 명명한다. CSI-A 기법을 구현하고 정적 및 동적 무선 환경에서의 실험을 통해 CSI-A 기법의 유용성과 한계를 규명한다.

2.3 IQ 불균형

동적 무선 환경에서 CSI-A 기법의 한계를 극복하기 위해, 송신 위치에 따라 변하는 CSI 값이 아닌 각 송신기 장치의 고유한 하드웨어 특성을 활용한 접근법이 필요하다. IQ 불균형은 이러한 하드웨어 특성 중 하나로, 무선 송신기 하드웨어에서 발생하는 미세한 불균형을 의미한다. 이는 I (In-phase) 신호와 Q (Quadrature) 신호 간 위상 및 진폭 차이가 완벽히 유지되지 못하여 발생하며, 각 송신기 장치마다 고유한 패턴을 가진다[15].

IQ 불균형은 진폭 불균형과 위상 불균형으로 두 가지로 구분되며, 본 논문에서는 분석의 용이성을 위해 각 불균형을 독립적으로 다룬다. 먼저, 진폭 불균형은 I_a로 정의하며, 단위는 dB이다. 진폭 불균형을 반영한 무선 채널 값 g는 다음과 같다.

$$g = g_r + jg_i,$$

여기서 $g_r = 10^{0.5I_a/20}$, $g_i = 10^{-0.5I_a/20}$이며 각각 실수부와 허수부의 오차를 나타낸다. 진폭 불균형이 클수록 g_r과 g_i 간의 차이가 증가하며 이는 전송 심볼의 성상도의 축 방향 이동을 초래한다.

위상 불균형은 I_p로 정의하며 단위는 degree이다. 위상 차이는 복소수 표현으로 다음과 같이 표현한다.

$$e^{j\theta},\ \theta = \pm\frac{0.5 \cdot I_p}{180} \cdot \pi$$

이때 θ는 위상 불균형으로 인해 발생하는 회전을 나타내며, $+\theta$와 $-\theta$는 각각 Q 신호와 I 신호에서의 위상 차이를 의미한다. 결과적으로 IQ 불균형이 적용된 수신 신호 y는 다음과 같이 정의된다.

$$y = g_r \angle(x) e^{-j\frac{0.5I_p}{180}\pi} + jg_i \angle(x) e^{+j\frac{0.5I_p}{180}\pi},$$

여기서 x는 송신 신호를 의미하며 $\angle(x)$는 송신 신호의 위상 값을 의미한다.

진폭 불균형은 g_r와 g_i의 차이를 통해 성상도의 이동을 초래하며, 위상 불균형은 θ를 통해 성상도의 회전을 발생시킨다. 예를 들어, 그림 5와 그림 6은 진폭 및 위상의 IQ 불균형이 수신 심볼의 성상도(constellation)에 미치는 영향을 나타낸다. 그림 5는 진폭 불균형의 영향을 보여주며, $I_a = 0$의 경우와 $I_a = 5$의 경우의 성상도 차이를 나타낸다. 그림 6는 위상 불균형의 영향을 보여주

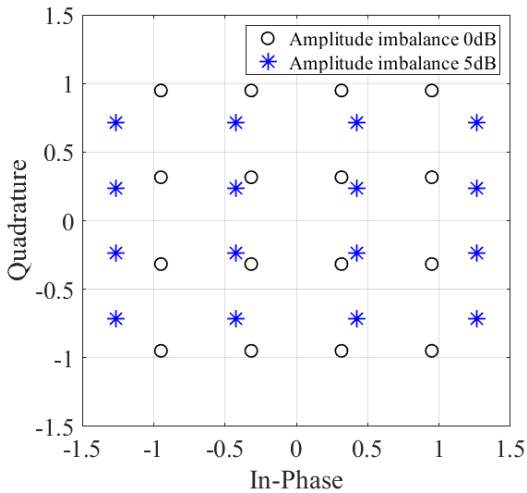

그림 5. IQ 불균형 예시(진폭)
Fig. 5. IQ imbalance example (amplitude)

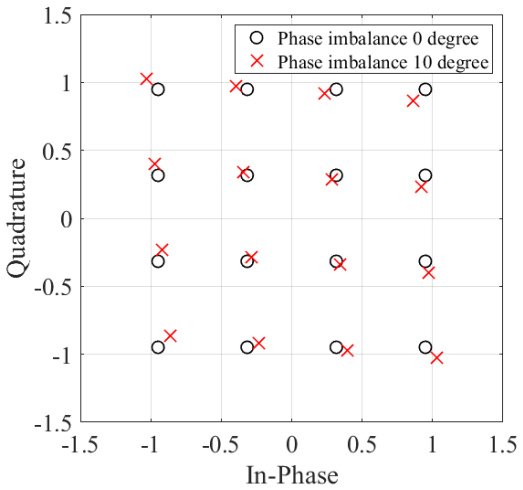

그림 6. IQ 불균형 예시(위상)
Fig. 6. IQ imbalance example (phase)

며, $I_p = 0$의 경우와 $I_p = 10$의 경우의 성상도 차이를 나타낸다. 이러한 IQ 불균형 특성은 하드웨어 고유의 차이를 반영하므로, 이를 기반으로 인공지능 모델을 학습시킴으로써 송신 위치와 관계없이 이블 트윈 공격을 효과적으로 탐지할 수 있다.

본 연구에서는 장치별 IQ 불균형에 따른 수신 신호 패턴을 학습하여 공격자를 탐지하는 CNN 기반 인증 기법을 제안한다. 본 논문에서 이러한 인증 기법을 IQ 불균형 기반 인증(IQ imbalance-based authentication 또는 IQ-A) 기법이라고 명명한다. 시뮬레이션을 통해 IQ-A 기법을 구현하고 IQ 불균형에 따른 공격자 탐지 정확도를 평가하여 송신 위치와 무관한 동적 디바이스 환경에서의 적용 가능성을 검증한다.

Ⅲ. CNN 기반의 물리계층 인증 기법

본 장에서는 CSI와 IQ 불균형 특성을 활용한 CNN 기반 물리계층 인증(PLA) 기법을 설명한다. 본 논문에서 고려하는 시스템 모델은 그림 7에 나타나 있으며, 합법적 AP와 이블 트윈 공격자로부터 수신한 신호의 고유한 특성(CSI 또는 IQ 불균형 값)을 기반으로 송신기를 분류한다. 수신기는 수신한 WLAN 신호에서 CSI 및 IQ 불균형과 같은 고유 특성을 추출한다. 추출한 특성은 데이터 전처리 과정을 거쳐 CNN 입력 데이터로 변환된다. CNN 모델은 훈련 과정을 통해 신호의 고유 특성을 학습하고 위장 공격 유무를 판단할 수 있게 된다.

본 연구에서는 CNN을 활용하여 위장 공격 탐지 모

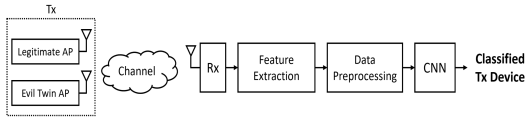

그림 7. 무선 신호 고유의 특성 기반 인증 시스템 모델
Fig. 7. Authentication system model based on unique characteristics of the wireless signal

델을 구현하였다. CNN은 이미지와 같은 공간적 특징을 학습하는 데 효과적이므로, 본 연구의 학습 데이터인 성상도와 같은 신호 표현에서 근접한 데이터 간 연관성을 학습하는 데 적합하다.

본 연구에서 사용한 CNN 모델의 구성은 표 2와 같다. CNN 입력 데이터는 (160×2×1)인 2차원 텐서로 구성되며 첫 번째 차원은 추출한 신호의 고유 특성 데이터를 기록한 길이를, 두 번째 차원은 I 신호와 Q 신호를 분리하여 표현한 값을 의미한다. 모델은 합성곱 계층, 배치 정규화 계층, 활성화 함수, 최대 풀링 계층, 완전 연결 계층, 드롭아웃 계층, 그리고 소프트맥스 계층으로 구성된다. 각 합성곱 계층은 배치 정규화를 포함한다. 합성곱 계층은 각각 필터 크기 (7×1)와 (7×2)를 사용하며, 필터 수는 50이다. 풀링 계층은 (2×1)의 풀 크기를 사용하며 활성화 함수는 ReLU를 사용한다. 첫 번째와 두 번째 완전 연결 계층에서 드롭아웃 비율은 0.5이며, 소프트맥스 계층을 통해 송신기 장치를 분류한다. 최적화 방법은 Adam을 사용하며 배치 사이즈는 256, 에포크는 12이다. 초기 학습률 0.001에서 학습이 진행됨에 따라 2 에포크마다 학습률이 절반으로 감소하는

표 2. CNN 모델 구조
Table 2. CNN model architecture

Layer	Layer Description	Output Size
Input	-	(160, 2, 1)
Conv_1	filters=50 kernel_size=(7, 1) ReLU Batch Normalization	(160, 2, 50)
Max_Pool_1	pool_size=(2, 1) stride=(2, 1)	(80, 2, 50)
Conv_2	filters=50 kernel_size=(7, 2) ReLU Batch Normalization	(80, 1, 50)
Max_Pool_2	pool_size=(2, 1) stride=(2, 1)	(40, 1, 50)
Dense_1	ReLU, Dropout=0.5	256
Dense_2	ReLU, Dropout=0.5	80
Dense_3	-	2

piecewise 스케줄 방식을 적용하였다.

3.1 CSI를 활용한 CNN 기반 PLA 기법

본 절에서는 CSI를 활용한 CNN 기반 인증 기법(CSI-A)을 소개한다. CNN 학습에 사용할 CSI 데이터는 IEEE 802.11 표준 규격에 기반한 구조를 사용한다. 물리 계층에서 사용되는 PPDU (physical protocol data unit) 프레임 구조에는 동기화 및 채널 추정을 위한 PLCP (physical layer convergence procedure) 프리앰블이 포함되며, 이 프리앰블 내의 L-LTF (long training field)는 채널 추정용 필드로 사용된다. L-LTF는 무선 채널의 특성을 분석하는 데 필요한 신호를 제공하며, 이를 기반으로 CSI를 얻을 수 있다. 본 연구에서는 그림 8과 같이 PPDU 포맷 중 Non-HT 프레임 구조의 L-LTF 필드에서 추출한 CSI 데이터를 수집하여 입력 데이터로 구성하며, CNN 모델은 이러한 CSI 데이터를 학습하여 위장 공격을 탐지한다.

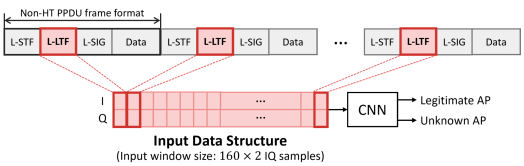

그림 8. CSI-A 기법을 위한 CNN 입력 데이터 구조
Fig. 8. CNN input data structure for CSI-A

3.2 IQ 불균형을 활용한 CNN 기반 인증 기법

본 절에서는 제안 기법인 IQ 불균형 특성을 활용한 CNN 기반 인증 기법(IQ-A)을 설명한다. IQ-A 기법에서 CNN 모델의 입력 데이터는 수신 신호의 성상도를 기반으로 구성한다. 수신 신호는 IQ 불균형의 영향을 포함하며, 송신기의 고유한 특성에 의해 결정된다. 수신 신호의 성상도를 I 신호와 Q 신호로 분리하여 CNN의 입력 데이터로 구성하였다. CNN 모델은 송신기의 고유 하드웨어 특성을 학습함으로써, 동적 무선 환경에서도 송신기를 탐지할 수 있다. 본 연구에서는 MATLAB을 활용해 IQ 불균형이 적용된 신호를 생성하였으며, 진폭 불균형과 위상 불균형에 따른 공격자 분류 정확도를 분석한다.

Ⅳ. 성능 평가

본 장에서는 CSI-A 기법과 IQ-A 기법의 성능 평가를 위한 실험 환경을 소개하고 실험 결과를 분석한다. 4.1절에서는 CSI-A 기법의 성능의 결과를 다루며, 정적 무선 환경과 동적 무선 환경에서 실제 WiFi 신호를 활용하여 공격 탐지 성능을 평가한다. 4.2절에서는 동일 환경에서 IQ-A 기법의 공격 탐지 성능 평가를 위한 MATLAB 기반 시뮬레이션 환경을 소개하고 실험 결과를 분석한다.

4.1 CSI-A 기법의 구현 및 성능 평가

CSI-A 기법의 성능 평가를 위해 정적 무선 환경과 동적 무선 환경에서 두 개의 ADALM-PLUTO SDR 장치를 활용하여 무선 신호 데이터를 생성 및 수집하고 실험을 진행하였다.

그림 9는 정적 무선 환경에서 CSI-A 기법의 실험 구성을 나타낸다. 합법적 AP 역할을 하는 송신기 SDR을 구현하고 신호를 수집하였다. 알 수 없는 송신기(Unknown)의 신호는 학습용으로 임의의 위치에서 생성 및 수집하였다. 수집한 신호에서 CSI와 MAC 주소를 추출한 후 전처리를 통해 CNN 모델의 학습 데이터로 구성하였다. 테스트 단계에서는 새로운 위치에서 SDR을 활용하여 이블 트윈 AP의 신호를 생성하였으며 이 신호는 합법적 AP의 MAC 주소를 위조한 형태를 가진다. 이블 트윈 AP 신호와 합법적 AP 신호를 CNN 모델에 입력하여 공격 탐지 성능을 평가하였다.

그림 10은 동적 무선 환경에서 CSI-A 기법의 실험 구성을 나타낸다. 본 실험은 동적 무선 환경에서 이블 트윈 AP가 합법적 AP와 근접한 위치로 이동하여 신호를 송신하는 시나리오를 가정한 것이다. 합법적 AP의 학습 데이터를 수집한 위치와 유사한 위치에서 공격자 신호를 송수신하여 테스트 데이터를 새롭게 생성한다. 생성한 테스트 데이터를 정적 무선 환경에서 학습된 모델에 입력하여 탐지 성능을 평가하였다. 이를 통해 CSI-A 기법이 동적 무선 환경에서도 합법적 AP와 공격자의 신호를 효과적으로 분류할 수 있는지 평가할 수 있다.

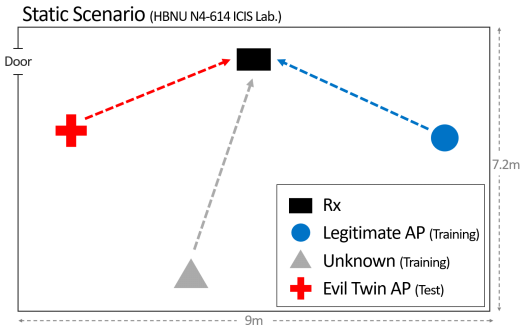

그림 9. CSI-A 기법 성능 평가 실험 환경(정적 환경)
Fig. 9. Experimental setting (static scenario)

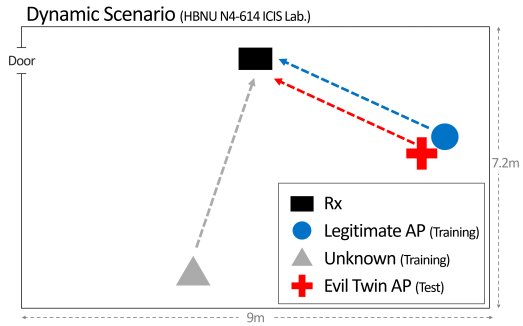

그림 10. CSI-A 기법 성능 평가 실험 환경(동적 환경: 공격자 AP 이동 가능)
Fig. 10. Experimental setting (dynamic scenario)

실험 결과는 표 3과 표 4에 정리된 결과와 같다. 표 3은 CSI-A 기법의 정적 무선 환경에서의 실험 결과를 나타낸다. 정적 무선 환경 실험에서는 학습 단계에서 합법적 AP와 Unknown 송신기의 신호를 학습하였으며, 테스트 단계에서는 학습 데이터 수집 시 합법적 AP의 위치와 서로 다른 위치에서 수집한 이블 트윈 공격자의 신호를 입력하여 성능을 평가하였다. 실험 결과, CSI-A 기법은 정적 무선 환경에서 99.3%의 높은 정확도로 위장 공격(이블 트윈 공격)을 탐지하는 것을 확인할 수 있다. 표 4는 CSI-A 기법의 동적 무선 환경에서의 실험 결과를 보여준다. 동적 무선 환경의 실험에서는 공격 탐지 정확도가 35%로 크게 감소하는 것을 확인할 수 있다. 합법적 AP와 근접한 위치에서 위장 공격(이블 트윈 공격)이 수행될 경우, CSI 값의 차별성이 감소하여 탐지 성능이 급격하게 저하되는 것을 확인할 수 있다.

표 3. 정적 디바이스 환경 실험 결과
Table 3. Experimental results of static device scenario

	Legitimate AP	Unknown
Legitimate AP	99%	1%
Unknown	0.7%	99.3%

표 4. 동적 디바이스 환경 실험 결과
Table 4. Experimental results of dynamic device scenario

	Legitimate AP	Unknown
Legitimate AP	99%	1%
Unknown	65%	35%

4.2 IQ-A 기법의 구현 및 성능 평가

IQ-A 기법의 구현과 성능 평가는 MATLAB을 활용한 컴퓨터 모의실험을 통해 수행하였다. IQ-A 기법의 성능을 평가하기 위해 QPSK와 16QAM 변조 방식을 사용하여 신호 데이터를 생성하고, 진폭 불균형(I_a) 및 위상 불균형(I_p)이 발생하는 시나리오에서 모의실험을 수행하였다. IQ-A 기법의 성능 평가를 위한 활용한 주요 파라미터는 표 5에 정리되어 있다. 학습 데이터로 합법적 AP 송신기와 임의의 알 수 없는 송신기(Unknown)의 신호를 구현하여 사용하였고, 테스트 데이터로 이블 트윈 공격자 송신기의 신호를 활용하였다. 각 송신기의 진폭 불균형 및 위상 불균형 조건을 달리하여 CNN 모델의 송신기 구분 성능을 평가하였다. 구체적인 실험 설계는 다음과 같다.

먼저 진폭 불균형에 따른 모의실험에서 합법적 AP의 데이터는 평균 I_a이 0인 신호로 구성하였으며, Unknown 송신기의 경우 평균 I_a이 각각 5, 10, 15인 신호를 생성하여 세 가지 독립적인 학습 데이터를 구성하였다. Unknown 송신기의 각 학습 데이터에 대해 개별적으로 CNN 학습을 수행하여 총 세 가지 CNN 모델을 생성하였다. 이를 QPSK와 16QAM 변조 방식 각각에 적용하여 최종적으로 여섯 개의 CNN 모델을 생성하였다. 테스트 데이터는 평균 I_a이 0,1,...,15인 이블 트윈 공격 신호를 사용하였다.

위상 불균형에 따른 모의실험은 진폭 불균형 실험과

표 5. IQ-A 기법 모의실험을 위한 주요 통신 파라미터
Table 5. Communication parameters for simulation of IQ-A

Parameter	Value		
Modulation scheme	QPSK, 16QAM		
# of frames	Training		3,600
	Test		2,000
Input frame length	160 samples		
IQ imbalance	Training	Legitimate AP	Amp.: $I_a = 0$ Phase: 0%
		Unknown	Amp.: $I_a = 5, 10, 15$ Phase: 25, 50, 75%
	Test	Evil Twin AP	Amp.: $I_a = 0, 1, \ldots, 15$ Phase: $0, 10, \ldots, 100\%$
Standard deviation of IQ imbalance	1dB		
SNR	15dB		

동일한 방식으로 여섯 개의 CNN 모델을 생성하였다. 위상 불균형은 $I_p = 0°$에서 $I_p = 180°$의 범위를 고려하였으며 이를 백분율로 변환하여 표현하였다. 즉, $I_p = 0°$은 위상 불균형이 0%, $I_p = 180°$는 위상 불균형이 100%이다. 합법적 AP의 위상 불균형은 0% ($I_p = 0°$)로 설정하였고, Unknown 송신기는 평균 위상 불균형이 각각 25%($I_p = 45°$), 50%($I_p = 90°$), 75% ($I_p = 135°$)로 설정하여 학습 데이터를 구성하였다. 각 Unknown 송신기 불균형 조건에 대해 QPSK와 16QAM 변조 방식을 적용하여 별도의 CNN 모델을 학습하였으며, 결과적으로 총 여섯 개의 CNN 모델을 생성하였다. 테스트 데이터는 이블 트윈 공격자 송신기의 신호를 활용하였으며, 평균 위상 불균형이 0%부터 100%까지 10% 간격으로 변화하는 신호를 생성하였다. 생성한 테스트 데이터를 여섯 개의 CNN 모델에 입력하여 공격자가 Unknown 송신기로 올바르게 분류되는 비율을 관찰하였다. 본 연구에서는 학습 데이터의 불균형 수준에 따라 생성된 모델을 구분한다. 예를 들어, $\mathrm{Model}_{\mathrm{I_a}}(0,5)$는 합법적 AP의 I_a가 0, Unknown 송신기의 I_a가 5인 경우에 대해 학습된 모델을 의미하며 $\mathrm{Model}_{\mathrm{I_p}}(0,50)$은 합법적 AP의 위상 불균형이 0%, Unknown 송신기의 위상 불균형이 50%인 경우에 대해 학습된 모델을 의미한다.

각 CNN 모델의 성능 평가는 학습된 모델에 이블 트윈 공격자 데이터를 입력하여 Unknown으로 올바르게 분류되는 비율을 기준으로 수행하였다. 특히, 공격자 신호가 Unknown 송신기와 서로 다른 불균형 평균값을 가질 때에도 모델이 높은 분류 성능을 유지할 수 있는지 검증하고자 하였다. 본 모의실험은 IQ-A 기법이 다양한 진폭 및 위상 불균형 환경에서 송신기 장치를 효과적으로 식별할 수 있는지 평가하는 것을 목적으로 한다.

그림 11은 이블 트윈 공격자의 진폭 불균형 수준에 따른 IQ-A 기법의 공격 탐지 정확도를 비교한 결과를 보여준다. 모의실험 결과, 학습한 불균형 수준 I_a에 가까운 테스트 데이터일수록 공격자를 Unknown으로 분류하는 정확도가 높아진다. 특히, 학습 시 합법적 AP ($I_a = 0$)와 Unknown 송신기의 불균형 수준의 차이가 클수록, 학습한 불균형보다 다소 낮은 불균형 수준에서도 최대 100%의 높은 정확도를 보임을 확인하였다. 이는 모델이 학습된 불균형 수준뿐만 아니라 일정 범위 내에서 일반화된 탐지 성능을 보임을 시사한다.

그림 12는 이블 트윈 공격자의 위상 불균형 수준에 따른 IQ-A 기법의 공격 탐지 정확도를 나타낸다. 모의

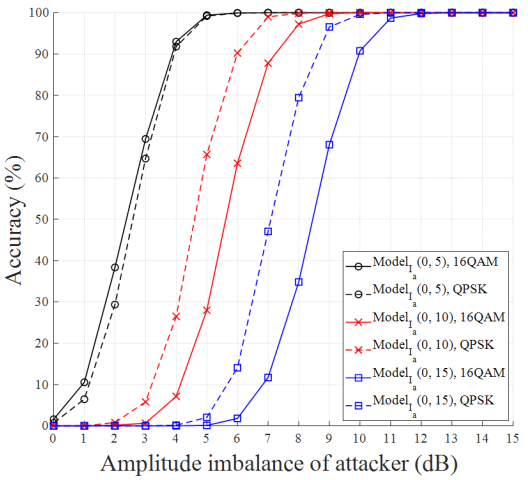

그림 11. 진폭 불균형 활용한 IQ-A 기법의 성능 평가: 학습 시 합법적 AP의 진폭 불균형(I_a)이 0이고, unknown 송신기의 I_a가 5, 10, 15일 때, $I_a = 0, 1, \ldots 15$인 공격자를 unknown으로 분류하는 비율

Fig. 11. Performance evaluation of IQ-A using amplitude imbalance: Percentage of attackers with $I_a = 0, 1, \ldots 15$ classified as unknown, when I_a of legitimate AP is 0 and I_a of unknown AP is 5, 10, 15 during training

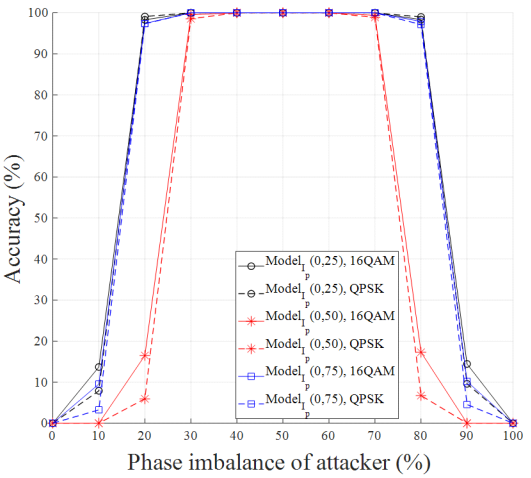

그림 12. 위상 불균형 활용한 IQ-A 기법의 성능 평가: 학습 시 합법적 AP의 위상 불균형(I_p)이 0%이고, unknown 송신기의 I_p이 25%, 50%, 75%일 때, I_p가 0%, 10%, ... 100%인 공격자를 unknown으로 분류하는 비율

Fig. 12. Performance evaluation of IQ-A using phase imbalance: Percentage of attackers with $I_p = 0\%, 10\%, \ldots 100\%$ classified as unknown, when I_p of legitimate AP is 0% and I_p of unknown AP is 25%, 50%, 75% during training

실험 결과, 학습한 위상 불균형 수준에 가까운 공격자 신호에 대해 높은 분류 정확도를 보였으며, 특히 학습 데이터와 동일한 위상 불균형 수준에서는 최대 100%의

분류 정확도를 보였다. 또한, $\mathrm{Model}_{I_p}(0,25)$과 $\mathrm{Model}_{I_p}(0,75)$은 비슷한 분류 성능을 보였는데, 이는 25%와 75%의 위상 불균형에서 생성된 성상도가 유사한 패턴을 가지기 때문으로 해석된다. 반면, $\mathrm{Model}_{I_p}(0,50)$은 30%에서 80%에 이르는 위상 불균형 범위에서도 95% 이상의 높은 분류 정확도를 유지하며, 우수한 일반화 성능을 보였다. 한편, 결과 그래프는 위상 불균형 0%에서 불균형 수준이 높아질수록 정확도가 상승한 후, 100%에 가까워질수록 점차 감소하는 형태를 보인다. 이는 위상 불균형 100%($I_p = 180°$)에서의 성상도가 위상 불균형 0%($I_p = 0°$)와 동일한 패턴을 보이므로 모델이 100% 불균형 신호를 합법적 AP ($I_p = 0°$)로 오인할 가능성이 높기 때문에 발생하는 결과이다.

V. 결 론

본 연구에서는 기존 WLAN 보안 프로토콜의 위장 공격(이블 트윈 공격) 취약성을 극복하기 위해 무선 신호의 고유한 특성을 활용한 물리계층 인증(PLA) 기법을 제안하고, 이를 검증하기 위한 실험 및 모의실험을 수행하였다. CSI 기반 인증 기법(CSI-A)은 채널 상태 정보(CSI)를 활용하여 합법적 송신기와 공격자를 분류하는 접근법으로, 정적 무선 환경에서 99.3%의 높은 공격자 분류 정확도를 보였다. 그러나 동적 무선 환경에서는 분류 정확도가 35%로 감소하여 위치 변화에 민감한 CSI의 한계를 확인하였다. 이를 보완하기 위해, 송신기 하드웨어의 고유 특성인 IQ 불균형을 활용한 IQ-A 기법을 제안하였다. 해당 기법은 송신기 위치와 관계없이 다양한 위상 및 진폭 불균형 환경에서 송신기를 최대 100%의 높은 공격 탐지 정확도를 보이며 IQ-A 기법의 유효성을 입증하였다. 향후 연구에서는 다양한 무선 환경과 실제 사용자 기기를 활용한 실험을 통해 제안 기법의 실질적인 적용 가능성을 검증하고, 보안 인증 성능을 더욱 향상시키는 방안을 모색하고자 한다.

References

[1] P. Porambage, et al., "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094-1122, May 2021. (https://doi.org/10.1109/OJCOMS.2021.3078081)

[2] M. Shi, et al., "IEEE 802.11 roaming and authentication in wireless LAN/cellular mobile networks," *IEEE Wireless Commun.*, vol. 11, no. 4, pp. 66-75, Aug. 2004. (https://doi.org/10.1109/MWC.2004.1325893)

[3] P. Satam and S. Hariri, "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 1, pp. 1077-1091, Mar. 2021. (https://doi.org/10.1109/TNSM.2020.3036138)

[4] D. Ficara, et al., "A tutorial on privacy, RCM and its implications in WLAN," *IEEE Commun. Surv. Tuts.*, vol. 26, no. 2, pp. 1003-1040, Dec. 2023. (https://doi.org/10.1109/COMST.2023.3345746)

[5] P. Shrivastava, et al., "EvilScout: Detection and mitigation of Evil Twin attack in SDN enabled WiFi," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 1, pp. 89-102, Mar. 2020. (https://doi.org/10.1109/TNSM.2020.2972774)

[6] N. Xie, et al., "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surv. Tuts.*, vol. 23, no. 1, pp. 282-310, Dec. 2020. (https://doi.org/10.1109/COMST.2020.3042188)

[7] K. Sankhe, et al., "ORACLE: Optimized radio classification through convolutional neural networks," in *Proc. IEEE INFOCOM-Conf. Comput. Commun.*, pp. 370-378, Paris, France, Apr. 2019. (https://doi.org/10.1109/COMST.2020.3042188)

[8] G. Shen, et al., "Radio frequency fingerprint identification for LoRa using spectrogram and CNN," in *Proc. IEEE INFOCOM 2021-Conf. Comput. Commun.*, pp. 1-10, Vancouver, Canada, May 2021. (https://doi.org/10.1109/COMST.2020.3042188)

[9] Y. Guo, et al., "Deep learning-enhanced physical layer authentication for mobile devices," in *Proc. IEEE GLOBECOM*, pp. 826-831, Kuala Lumpur, Malaysia, 2023.

(https://doi.org/10.1109/COMST.2020.3042188)

[10] Q. Wang, et al., "Spatiotemporal gradient-based physical-layer authentication enhanced by CSI-to-image transformation for industrial mobile devices," *IEEE Trans. Ind. Inf.*, vol. 20, no. 3, pp. 4236-4245, Mar. 2024. (https://doi.org/10.1109/TII.2023.3316178)

[11] R. Xie, et al., "Disentangled representation learning for RF fingerprint extraction under unknown channel statistics," *IEEE Trans. Commun.*, vol. 71, no. 7, pp. 3946-3962, Jul. 2023. (https://doi.org/10.1109/TCOMM.2023.3268286)

[12] L. Yang, et al., "On the use of power amplifier nonlinearity quotient to improve radio frequency fingerprint identification in time-varying channels," in *Proc. IEEE Annu. Int. Symp. PIMRC*, pp. 1-7, Toronto, ON, Canada, 2023. (https://doi.org/10.1109/PIMRC56721.2023.10293946)

[13] N. Basha, et al., "Leveraging MIMO transmit diversity for channel-agnostic device identification," in *Proc. IEEE ICC*, pp. 2254-2259, Seoul, South Korea, 2022. (https://doi.org/10.1109/ICC45855.2022.9838976)

[14] J. He, et al., "Radio frequency fingerprint identification for OFDM system considering unknown multipath fading channel," *IEEE Trans. Cogn. Commun. Netw.*, vol. 10, no. 6, pp. 2076-2087, Dec. 2024. (https://doi.org/10.1109/TCCN.2024.3405481)

[15] A. Tarighat, et al., "Compensation schemes and performance analysis of IQ imbalances in OFDM receivers," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 3257-3268, Aug. 2005. (https://doi.org/10.1109/TSP.2005.851156)

오 한 올 (Hanol Oh)

2025년 2월 : 국립한밭대학교 정보통신공학과 (공학사)

<관심분야> 5G/6G, 무선통신 시스템, 머신러닝/인공지능

[ORCID:0009-0003-0198-3459]

윤 지 현 (Jihyeon Yoon)

2025년 2월 : 국립한밭대학교 정보통신공학과 (공학사)

2024년 12월~현재 : 세림티에스지(주) 사원

<관심분야> 무선네트워크 보안, 이동통신 보안, 인공지능

[ORCID:0009-0004-3804-1331]

문 지 환 (Jihwan Moon)

2014년 2월 : 고려대학교 전기전자전파공학부 (공학사)

2019년 2월 : 고려대학교 전기전자공학과 (공학박사)

2019년 3월~2019년 7월 : 고려대학교 정보통신기술연구소 연구교수

2019년 7월~2020년 8월 : 국가보안기술연구소 연구원

2020년 9월~2022년 2월 : 조선대학교 정보통신공학부 조교수

2022년 3월~현재 : 국립한밭대학교 모바일융합공학과 조교수

<관심분야> Optimization techniques, energy harvesting, physical-layer security, wireless surveillance, covert communications, and machine learning for wireless communications

[ORCID:0000-0002-9812-7768]

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~2022년 9월 : 국립한밭대학교 컴퓨터공학과 조교수
2022년 10월~현재 : 국립한밭대학교 컴퓨터공학과 부교수
<관심분야> Wireless Communications, Satellite Communications, Wireless Network Security
[ORCID:0000-0001-7109-1999]

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~2022년 9월 : 국립한밭대학교 정보통신공학과 조교수
2022년 10월~현재 : 국립한밭대학교 지능미디어공학과 부교수
<관심분야> 6G/5G, 무선네트워크보안, 이동통신보안, 물리계층보안, 위성통신, 인공지능 무선통신 응용
[ORCID:0000-0001-7109-1999]