물리계층 보안기술 동향

Trends in Physical Layer Security Technologies

김대원 (D.W. Kim, dwkim77@etri.re.kr) 암호공학연구실 책임연구원
윤승용 (S.Y. Yoon, syyoon@etri.re.kr) 암호공학연구실 책임연구원
강유성 (Y.S. Kang, youskang@etri.re.kr) 암호공학연구실 책임연구원
김병구 (B.K. Kim, bkkim05@etri.re.kr) 암호공학연구실 책임연구원/실장

ABSTRACT

Physical layer security (PLS) provides a complementary approach to securing wireless communications by leveraging intrinsic physical properties of channels and radio signals. As wireless systems move toward massive connectivity, heterogeneous architectures, and dynamic environments, including the Internet of Things, satellite communications, and future 6G networks, conventional cryptographic mechanisms face growing limitations in scalability, complexity, and long-term resilience. This article surveys recent PLS technologies, focusing on secret key generation and physical layer authentication based on channel- and device-specific features. It classifies representative probing signals by implementation requirements, environmental suitability, and security performance. It also reviews recent advances in artificial intelligence-assisted PLS and reconfigurable intelligent surface-enabled security. The review shows that these approaches can enhance channel randomness, robustness, and resistance to emerging attacks. It identifies key challenges and research directions for intelligent, adaptive security frameworks.

KEYWORDS Information Security, Physical Layer Security, Secret Key Generation, Wireless Security

I. 서론

차세대 이동통신, 사물인터넷(IoT: Internet of Things), 위성통신, 자율주행 및 국방 · 공공 통신망 등 무선통신 기반 서비스가 급속히 확산함에 따라, 통신 시스템의 보안성은 기존보다 훨씬 중요한 요소로 주목받고 있다. 특히 무선통신은 전송 매체의 개방성으로 인해 도청(Eavesdropping), 전파방해(Jamming), 스푸핑(Spoofing) 등 다양한 공격에 본질적으로 취약하며, 이는 기존의 암호 기반 상위 계층 보안 기술만으로는 근본적인 대응에 한계가 있다.

이러한 배경에서 물리계층 보안(PLS: Physical Layer

* DOI: https://doi.org/10.22648/ETRI.2026.J.410504
* This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) [No. RS-2024-00360387, Development of core security technology utilizing multi-modal properties of wireless communication channels].

본 저작물은 공공누리 제4유형
출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.
©2026 한국전자통신연구원

Security)은 통신채널의 물리적 특성과 신호 처리 기법을 활용하여 정보의 기밀성, 무결성, 및 가용성을 확보하는 기술로 주목받고 있다. 물리계층 보안기술은 연산 복잡도가 높은 암호 알고리즘에 의존하지 않고, 채널 잡음, 페이딩, 다중경로, 안테나 특성 등 물리적 특성을 활용함으로써 정보 이론적으로 안전한 통신을 구현할 수 있다는 장점이 있다. 또한, 경량 보안이 요구되는 IoT 단말이나 실시간성이 중요한 무선 시스템에 적합한 대안으로 평가받고 있다.

최근에는 다중 안테나(MIMO: Multiple-Input Multiple-Output) 기술, 빔포밍(Beamforming), 인공 잡음(Artificial Noise), 비밀키 생성(Secret Key Generation), RF 지문(RF Fingerprinting), 재구성 지능형 표면(RIS: Reconfigurable Intelligent Surface) 등과 결합된 물리계층 보안기술이 활발히 연구되고 있으며, 물리적 특성 분석에 인공지능(AI: Artificial Intelligence) 및 머신러닝(ML: Machine Learning) 기술이 접목되고 있다. 특히 6G 통신, 위성-지상 통합 네트워크, 저궤도(LEO: Low Earth Orbit) 위성 환경 등 새로운 통신 패러다임에서는 물리계층 보안의 역할이 더 확대될 것으로 전망된다.

본고에서는 이러한 기술적, 환경적 변화에 대응하여, 물리계층 보안기술 배경 및 최근 연구들을 소개한다. 이를 통해 향후 무선통신 시스템에서 물리계층 보안기술이 차지하는 기술적 의미와 발전 방향을 조망한다.

II. 물리계층 보안기술 배경

본 장에서는 물리계층 보안기술 배경정보로서 무선통신 보안환경의 변화, 물리계층 보안기술의 개념, 및 물리계층 특성 기반 공통정보 생성 절차 등을 소개한다.

1. 무선통신 보안환경의 한계 및 변화

물리계층 보안기술은 과거 이론 중심의 연구가 진행된 후, 실용적 부분에서는 기술적인 한계로 한동안 진척이 없었으나, 최근 몇 년 사이 차세대 무선통신 환경과 인공지능/머신러닝 기반 신호 처리 기술의 발전을 계기로 기술 응용 관점에서 재조명되고 있다.

표 1은 물리계층 보안기술 연구 및 관심 변화 추이를 보여준다. 기존의 보안 통신 환경에서는 사전에 공유된 암호키(PSK: Pre-Shared crypto Key)나 공개키 기반 키 교환 또는 키 캡슐화 메커니즘을 이용한

표 1 물리계층 보안기술 연구환경 변화

구분	시기	주요 특징	핵심 배경 및 이슈
초기 이론 정립 및 연구 활성기	2008~2015년	• 정보이론 기반 물리계층 보안 이론 정립 • Wiretap Channel, Secrecy Capacity 연구 활발 • MIMO, 협력 통신, Artificial Noise 기법 제안	• 무선 채널의 물리적 특성 활용 가능성 제시 • 이론적 성능 분석 중심 연구 • 실제 시스템 적용은 제한적
관심 감소 및 정체기	2016~2019년	• 연구 규모 및 실용적 관심 감소 • 제한적 응용 사례 중심 연구 지속	• 기존 암호 기술의 실용적 안정성 확보 • 채널 가정의 비현실성 문제 • 표준화·상용화 어려움
재부상 및 실용화 지향 연구 확대	2020년 이후	• 차세대 무선 환경 중심으로 연구 재활성화 • AI/ML 기반 물리계층 보안기술 등장 • RIS, massive MIMO 등과 결합	• IoT·초연결·저궤도 위성 환경 확산 • 암호키 관리 확장성 한계 부각 • 양자 컴퓨팅 위협 대응 필요성 • 다계층 보안 패러다임 확산

암호키 공유 방식이 주로 사용되어 왔다. 이러한 방식은 다양한 통신 시스템에서 기밀성을 확보하는 데 효과적이지만, 키 분배 및 관리 인프라의 복잡성, 대규모 네트워크 환경에서의 확장성 한계, 연산 복잡도에 따른 성능 저하, 그리고 양자 컴퓨팅 기술 발전에 따른 암호 알고리즘의 안전성 위협 등의 문제점이 점차 부각되고 있다.

특히 사물인터넷, 초연결 네트워크, 저궤도 위성, 및 이동통신 시스템 등과 같이 단말 수가 급증하고 동적 토폴로지를 가지는 무선 환경에서는 기존 암호 기반 키 관리 방식의 적용이 더욱 어려워지고 있다. 제한된 연산 능력과 전력 자원을 갖는 단말에서는 공개키 연산에 따른 부담이 크며, 중앙 집중형 키 관리 구조는 시스템 유연성과 신뢰성을 저하시킬 수 있다. 또한, 양자 컴퓨팅의 발전은 기존 공개키 암호체계의 장기적 안전성에 대한 근본적인 재검토를 요구하고 있다.

한편, 기존 물리계층 보안기술 및 무선 신호 분석 기법은 전문가의 수작업 설계와 규칙 기반 신호 처리 알고리즘에 크게 의존해 왔으며, 이는 복잡하고 동적인 무선 환경에서 채널 특성 변화, 비선형 왜곡, 환경 의존적 특성을 충분히 반영하는 데 한계를 가진다. 특히 고차원 신호 특성이나 시간 · 주파수 · 공간 영역의 복합적인 상관관계를 수작업으로 모델링하는 데는 명확한 제약이 존재한다.

이러한 한계를 극복하기 위해 최근에는 인공지능 및 머신러닝 기술을 물리계층 보안기술에 접목하려는 연구가 활발히 진행되고 있다. AI 기반 기법은 복잡한 무선 채널 환경에서 신호의 통계적 · 구조적 특성을 자동으로 학습할 수 있으며, 채널 추정, 비밀키 생성, 사용자 인증, 공격 탐지 등 다양한 물리계층 보안 기능의 성능을 향상시키는 데 이바지하고 있다. 이를 통해 기존의 암호 기반 보안기술을 보완함과 동시에, 무선 환경 적응형 · 지능형 보안 메커니즘을 구현할 새로운 가능성이 제시되고 있다. 이에 따라 차세대 무선통신 환경을 중심으로 AI 기반 물리계층 보안기술에 관한 연구와 관심이 지속적으로 확대되고 있다.

2. 물리계층 보안기술 개념

그림 1은 물리계층 보안기술의 개념을 보여준다 [1]. 그림에서 Alice와 Bob은 합법적인 통신 주체이며, 동일한 무선 전파 환경에서 높은 상관성을 갖는 무선 채널(Highly Correlated Wireless Channel)을 공유한다. 이는 무선 채널의 상호성(Channel Reciprocity) 특성에 기인하며, Alice와 Bob이 시간상으로 거의 동시에 채널을 측정할 경우 유사한 채널 응답을 얻을 수 있음을 의미한다.

반면, 도청자 Eve는 Alice-Bob과 물리적으로 다른 위치에 존재하므로, 다른 전파 경로에 의한 공간 비상관(Spatial Decorrelation) 특성에 의해 Alice-Bob 채널과 상관성이 낮은 채널을 관측하게 된다. 이에 따라 Eve가 관측한 채널 정보는 Alice와 Bob이 공유하는 채널 정보와 일치하지 않으며, 이를 기반으로 생성되는 비밀 정보(예: 암호키)를 추정하기 어렵다.

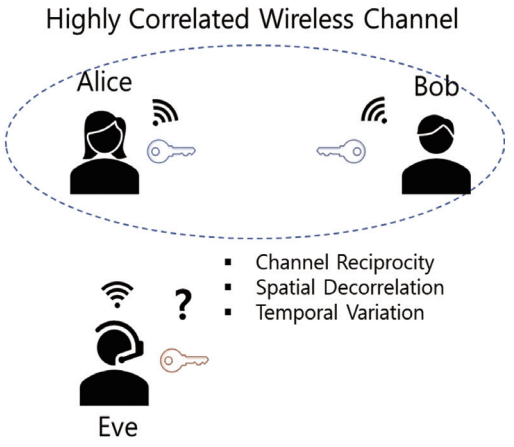


그림 1 물리계층 보안기술 개념도

또한, 무선 채널은 사용자 이동, 환경 변화 등에 따라 지속적으로 변화하는 시간적 변동성(Temporal Variation)을 가지며, 이러한 무작위성(Randomness)은 물리계층 보안기술에서 비밀 정보를 생성하기 위한 중요한 엔트로피 원천으로 활용된다.

결과적으로, 물리계층 보안기술은 ① 채널 상호성을 통해 합법 사용자 간 높은 채널 유사성을 확보하고, ② 공간 비상관 특성을 통해 도청자의 정보 획득을 제한하며, ③ 채널의 시간적 변동성을 이용해 비밀 정보를 생성함으로써 추가적인 암호 연산 없이도 무선통신의 기밀성을 강화하는 보안 메커니즘을 제공할 수 있다.

3. 물리계층 특성기반 공통정보 생성 절차

물리계층 보안기술 개념을 이용하여, 두 무선통신 기기 간 공통 채널 정보 및 기기 고유정보를 생성하는 것이 이론적으로 가능하다. 전자는 암호키 생성, 후자는 기기 인증 등에 응용된다. 본 절은 물리계층 수집정보를 이용한 공통 채널 정보 생성 절차를 소개한다. 이 절차는 암호키 생성 및 기기 인증 등에 활용될 수 있다.

그림 2는 무선 환경에서의 물리계층 특성 기반 공통정보 생성 절차[2]를 시스템적으로 정리한 것으로, 이후 많은 서베이와 논문 등에서 재사용되고 있는 방식이다. 다음에서 이 방식을 이용한 암호키 생성 예를 소개한다.

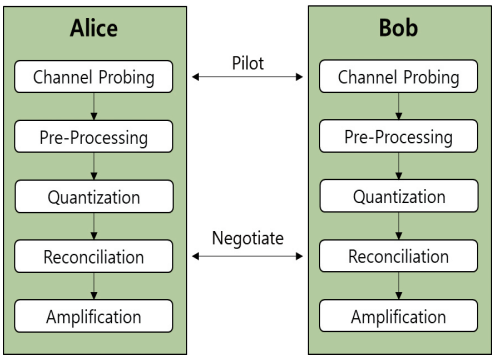


그림 2 물리계층 특성기반 공통정보 생성 과정

그림 2에서는 Alice와 Bob이 동일한 암호키를 생성하는 절차를 단계적으로 보여준다. 해당 절차는 무선 채널의 상호성과 무작위성을 활용하여, 사전에 암호키를 공유하지 않고도 안전한 키 합의를 가능하게 한다.

3.1 Channel Probing

Alice와 Bob은 파일럿(Pilot) 신호를 상호 교환하며 무선 채널을 측정한다. 이 과정에서 두 단말은 시간상으로 거의 동시에 동일한 무선 채널을 관측하게 되며, 이로부터 수신 신호 세기(RSSI: Received Signal Strength Indicator), 채널 상태 정보(CSI: Channel State Information) 등의 물리계층 채널 정보를 획득한다. 채널 상호성에 의해 양측이 관측한 채널 정보는 높은 상관성을 가진다.

3.2 Pre-processing

측정된 채널 정보에는 잡음, 하드웨어 불일치, 비동기성 등으로 인한 오차가 포함되므로, 이를 보정하기 위한 전처리 과정이 수행된다. 평균 제거, 필터링, 정규화 등의 기법을 통해 채널 특징을 추출하고, Alice와 Bob 간 채널 상호성을 강화함으로써 이후 단계에서의 키 불일치를 최소화한다.

3.3 Quantization

전처리된 아날로그 형태의 채널 측정값을 디지털 비트열로 변환하는 양자화(Quantization)를 수행하고, 이를 기반으로 암호키 생성에 활용할 공통 비트열을 생성한다. 이 단계에서 양자화 방식 및 임계값 설정은 키 생성률과 키 불일치율에 직접적인 영향을 미친다.

3.4 Reconciliation

채널 측정 오차로 인해 Alice와 Bob이 생성한 공통 비트열에는 일부 불일치가 발생할 수 있으므로, 공개 채널을 통해 오류 정정을 수행한다. 이 과정에서는 패리티 정보 등 최소한의 보조 정보만 교환되며, 실제 비트열은 노출되지 않는다. 비트열의 해시된 정보를 송수신하여 비교하는 방식이 대표적이다.

3.5 Amplification

정보 조정(Reconciliation) 과정에서 누설될 수 있는 정보를 제거하고 필요한 암호키 길이 등으로 가공하기 위해, 해시 함수 등의 기법을 적용한 최종 암호키를 생성한다. 이를 통해 도청자(Eve)가 일부 정보를 획득하였더라도 최종 키를 추정하는 것은 정보이론적으로 불가능하게 한다.

III. 물리계층 보안기술 관련 연구

Ⅱ장에서 설명된 배경지식을 바탕으로, 본 장에서는 물리계층 보안기술 관련 신호종류별 특징, 전통적인 분석 기반, AI/ML 기반, 및 RIS 기반 등의 연구들을 소개한다. 이 연구들은 다방면의 무선통신에 활용될 수 있으며, 특히 기존 암호체계 수준 이상의 통신보안이 요구되는 특수목적 통신(국방, 우주 등) 등에 응용될 수 있다.

1. 신호종류별 특징 분류

물리계층 보안기술에서 고려할 사항 중 하나는, 키 생성(PKG: Physical layer Key Generation)이나 기기 인증(PLA: Physical Layer Authentication) 등 목적에 따라 어떤 신호 특징을 Probing 할 것인지에 관한 결정이다.

표 2는 Probing 신호종류별 특징들을 보여준다. 구분은 신호종류를 나타내며, 해당 신호를 이용한 관련 논문들이 참조되어 있다. 신호 활용 목적에 따라 RSS, CIR(Channel Impulse Response), CFR(Channel Frequency Response), CSI, Transient Amplitude(신호 송출/종료 시점의 짧은 진폭 패턴), CFO(Carrier Frequency Offset), Phase Noise, I/Q(In-Phase/Quadrature) Imbalance 등이 주로 수집된다. 표 3은 사용환경별 적합한 신호종류들을 정리하였으며, 표 4는 보안 관점에서 신호종류별 특징을 보여준다. 최근 무선 신호의 다중(Multi-Modal) 특징 반영을 위해, PKG에는 CSI, PLA

표 2 Probing 신호종류별 특징 분류

구분	특징 정보	정보 도메인	시간적 안정성	공간 의존성	구현 복잡도	주요 활용
RSS[3]	수신 신호 세기	시간	중	높음	낮음	PKG/PLA
CIR[4]	다중경로 임펄스 응답	시간	중~낮음	매우 높음	중	PKG/PLA
CFR[5]	주파수 응답	주파수	중	높음	중	PKG
CSI[6]	채널 이득 (진폭·위상)	시간·주파수·공간	낮음	매우 높음	높음	PKG
Transient Amplitude[7]	송신 과도 특성	시간	매우 높음	낮음	중	PLA
CFO[8]	주파수 오프셋	주파수	높음	낮음	낮음	PLA
Phase Noise[9]	위상 잡음	주파수	높음	낮음	중	PLA
I/Q Imbalance[10]	I/Q 비대칭	복합	매우 높음	낮음	중	PLA

표 3 환경별 적합 Probing 신호종류

환경	적합 신호종류	이유
IoT 저전력	RSS, CFO	연산·전력 부담 낮음
고이동성	CFO, Phase Noise	시간 안정성 높음
실내 정적 환경	CIR, CSI, CFR	공간 분해능 우수
수중 통신	CIR, CSI, CFR	채널 특성 풍부
위성	CFO, CSI, CFR	Doppler·빔 특성 활용
기기 기반 인증	Transient Amplitude, I/Q Imbalance	하드웨어 고유성

표 4 보안 관점의 Probing 신호종류별 특징

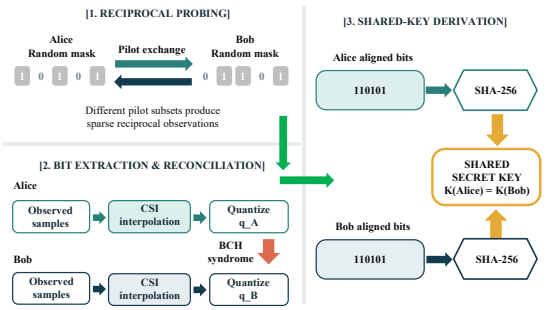
구분	랜덤성	고유성	재현성	도청자 분리성	주요 공격대응
RSS	중	낮음	중	중	도청
CIR	높음	중	중	높음	
CFR	중	중	중	높음	
CSI	매우 높음	중	낮음	매우 높음	
Transient Amplitude	낮음	매우 높음	높음	매우 높음	기기 위조
CFO	낮음	높음	높음	높음	
Phase Noise	낮음	높음	높음	높음	
I/Q Imbalance	낮음	매우 높음	매우 높음	높음	

에는 I/Q Imbalance 적용 등을 고려해 볼 수 있다.

2. 전통적인 분석기반 물리계층 보안연구

본 절에서는 주로 알고리즘 구현을 통한 전통적인 방식으로 무선 신호 특징 분석을 수행하는 최근 연구들을 소개한다.

그림 3에서 Kojima 등[11]은 Alice와 Bob이 사전 공유정보 없이, 파일럿(Pilot)을 랜덤하게 감소시켜 도청자(Eve)의 채널 추정을 어렵게 만드는 것을 핵심으로 하는 비밀키 생성(SKG: Secret Key Generation) 방법을 제안한다.



출처 Author-created conceptual workflow of physical layer secret key generation using randomized pilot activation. The procedural concepts are summarized from [11].

그림 3 무작위 감소 기반 SKG

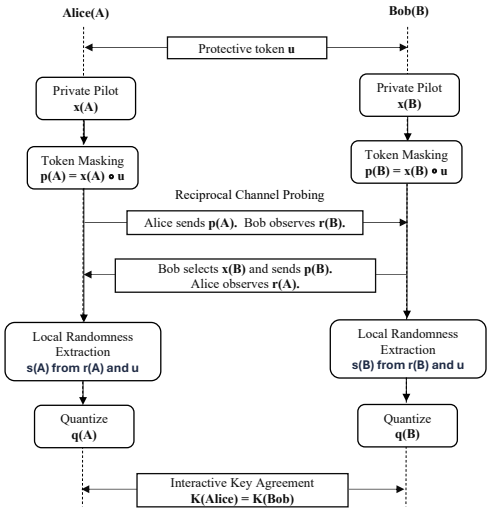
Random Pilot Reduction 단계에서, Alice와 Bob은 각자 파일럿 심볼의 일부를 동일한 감소비율로 비활성화하고, 어떤 파일럿이 제거되었는지는 외부에 공개하지 않는다. Alice와 Bob은 감소된 파일럿 신호로부터 부분적인 CSI를 Probing한다. 랜덤하게 제거된 파일럿으로 인해 CSI가 불완전하므로, 보간(Interpolation) 기법을 사용해 전체 CSI를 복원한다. 복원된 CSI(RSS 기반)의 양자화(Quantization)에는 불안정한 샘플은 폐기하고 키 불일치율은 감소시키기 위한 가드 밴드 기반 임계값을 적용한다. Reconciliation 단계에서 Alice는 패리티 정보만 공개 채널로 Bob에게 전송하며, Bob은 이를 이용해 오류를 수정한다. SHA-256 해시 함수를 적용하여 누설 가능 정보를 제거한 최종 공유 비밀키(Shared Secret Key)를 생성한다.

Wu 등[12]은 기존 물리계층 암호키 생성에 사용되던 공개 파일럿 기반 채널 랜덤성 교환 구조를 확장하여, 파일럿 자체를 보호 토큰(Protective Secret Token)으로 은닉하고 랜덤성 교환 단계에서 도청자의 관측 구조를 근본적으로 방해하는 새로운 보안 패러다임을 제시한다. 그림 4는 제안 기법이 채널 랜덤성을 생성하는 단계 이전부터 공격 표면을 제거함으로써, 내부 도청자 환경에서도 안전한 물리

계층 암호키 생성을 가능하게 함을 설명한다.

그림 4에서는 기존의 DH-SKG(Diffie-Hellman-based SKG)가 내부 도청자(Internal Eavesdropper)에 취약하다는 문제를 해결하기 위해, 보호 토큰을 이용하여 채널 무작위성을 은닉하는 과정을 보여준다. Alice와 Bob은 각각 개인 파일럿(Private Pilots)을 생성한 후, 사전에 공유된 비밀 정보를 기반으로 생성한 보호 토큰 u(k)을 이용하여 파일럿 신호를 은닉한다. 즉, 송신되는 파일럿은 단순한 공개 파일럿이 아니라, 토큰이 곱해진 형태로 전송된다.

Alice와 Bob은 수신 신호를 자신이 알고 있는 파일럿과 보호 토큰으로 역처리함으로써 토큰이 제거된 형태의 채널 랜덤 시퀀스를 복원한다. 이 과정에서 양측은 채널 상호성에 의해 높은 상관성을 갖는 공통 무작위성을 확보할 수 있으며, 이는 이후 양자화 및 키 합의 단계에 사용된다. 도청자는 보호 토큰 u(k)를 알 수 없기 때문에 수신 신호를 재구성하더라도 토큰이 제곱 형태(u^2)로 남은 왜곡된 랜덤 시퀀스를 관측하게 된다. 논문에서는 토큰의 위상을 균등



출처 Author-created conceptual workflow of token-protected physical layer secret key generation through reciprocal probing. The procedural concepts are summarized from [12].

그림 4 보호토큰 기반 SKG

분포로 설계하여, 도청자가 획득한 랜덤 시퀀스와 합법 사용자 간 랜덤 시퀀스 사이의 상관관계가 이론적으로 0이 됨을 보인다.

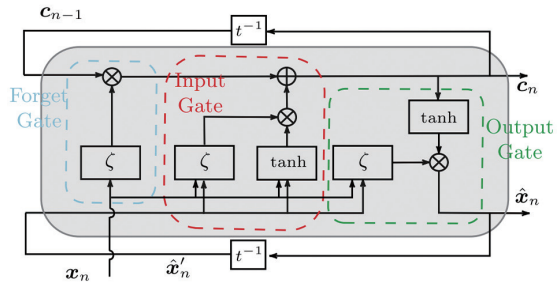
3. AI/ML 기반 물리계층 보안연구

본 절에서는 인공지능 및 머신러닝 기술이 접목된 물리계층 보안기술 관련 최근 연구들을 소개한다. 전통적인 분석방법으로는 설계 및 구현이 어려운 비선형적이거나 복잡한 관계를 포함하는 특징들을 통합하여, 암호키 생성 및 기기 인증을 위한 특정한 범위값들이나 고유값들을 유도할 수 있다. 물리계층 보안기술이 다시 관심받게 된 주된 이유 중 하나이다.

Ardizzon 등[13]은 잠수함 등의 수중환경에 적용할 수 있는, 다수 센서와 분산 예측기(Predictor)를 활용한 물리계층 인증 시스템의 전체 구조 및 통신채널 특성의 시간적 진화(Evolution)를 학습하기 위한 LSTM(Long Short-Term Memory) 기반 예측기 구성을 제안하였다.

수중 음향 채널은 느리지만 지속적으로 변화하여 단순 통계 기반 인증은 성능저하가 수반되므로, 채널 특성의 시간적 연속성을 학습할 필요가 있다. 그림 5와 같이 과거 상태 중 유지/삭제할 정보 결정(Forget Gate), 현재 입력 채널 특성(Input Gate) 및 현재 시점의 예측값 출력(Output Gate)을 통해, 급변하거나 이동성이 높은 무선 환경에서도 채널 특성의 시간적 패턴을 안정적으로 예측할 수 있다. 예측 오차가 사전에 설정된 임계값 이하일 경우, 송신자를 합법적인 사용자로 판단한다.

Elmaghbub 등[14]은 RF 지문을 구성하는 하드웨어 결함(Hardware Impairments)이 장치의 전원 인가 이후 워밍업 과정에서 시간에 따라 비정상적으로 변동하며, 특히 CFO와 SCE(Symbol Clock Error)와 같



출처 Reprinted from F. Ardizzon et al., "A RNN-Based Approach to Physical Layer Authentication in Underwater Acoustic Networks with Mobile Devices," Comput. Netw., vol. 243, no. 110311, 2024. doi: 10.1016/j.comnet.2024.110311.

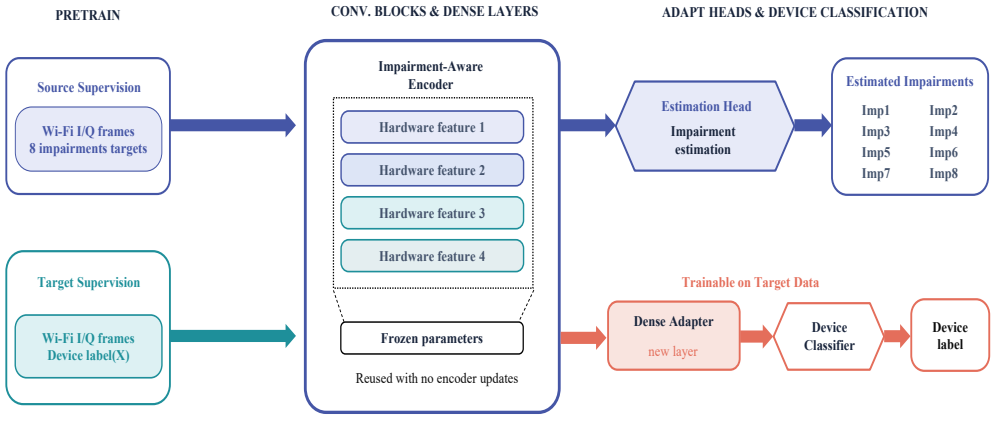
그림 5 예측기로 사용된 LSTM cell 특성

은 결함이 초기 구간에서 큰 변화를 보임으로써 기존 딥러닝 기반 RF 지문 인식 성능이 급격히 저하될 수 있음을 체계적으로 분석하였다.

RF 지문을 단일 신호 패턴이 아닌 다수의 하드웨어 결함 성분으로 분해하여, 워밍업 전 · 후 단계에서 각 결함이 신호에 미치는 영향과 딥러닝 모델의 특징 학습 양상이 어떻게 달라지는지를 정량적으로 관찰한다. 이를 바탕으로, 그림 6과 같이 신호로부터 장치 고유의 하드웨어 결함을 직접 추정하는 사전 학습 단계와 해당 결함 표현을 기반으로 장치 식별을 수행하는 순차적 전이 학습(Sequential Transfer Learning)을 결합한 HEEDFUL(Hardware-Enhanced Embedding for Device Fingerprinting with seqUential Learning) 프레임워크를 제안하였다. 제안된 기법은 안정화 이후 구간에서 기존 모델의 블라인드 스팟(특정 구간 오분류) 문제를 구조적으로 해소하며, 워밍업 구간을 포함한 다양한 조건에서도 일관된 장치 식별 성능을 유지함을 실험적으로 입증하였다.

4. RIS 기반 물리계층 보안연구

3GPP Release 18~19 과정에서, RIS는 표준화 검토 후보로 제안되었으나 정식 study item으로 이어지지는 않았으며, 채널 모델링, CSI 측정/피드백, 빔 관리 등 향후 6G 후보 기술로 연구가 지속되고 있다. 삼성, 화웨이, 에릭슨, 노키아, 퀄컴 등과 다수의 연구 기관에서 5G RIS 실증 시험과 프로토타입을 수행하고 있으나, 현재 상용 5G 이동통신망에서는 RIS가 일반 서비스 기능으로 도입된 사례는 제한적이다. 반면, 6G 기술 로드맵에서는 Terahertz 및 초고주파 대역의 전파 환경에서 RIS가 중요한 역할을 할



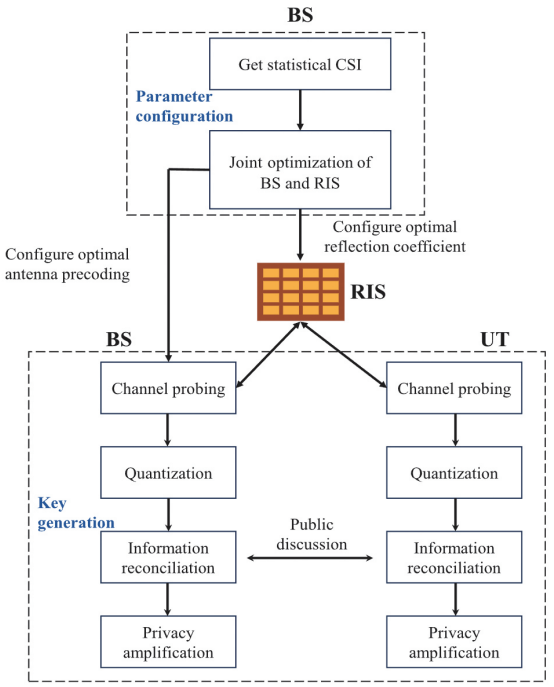
출처 Author-created conceptual workflow of sequential transfer learning in HEEDFUL for Wi-Fi device classification. The procedural concepts are summarized from [14].

그림 6 HEEDFUL의 학습 절차 개념도

가능성이 높으며, 인공지능 기반 최적화와 결합함으로써 환경 적응성, 에너지 효율성, 공간 다중화 측면에서 핵심 역할을 할 것으로 전망된다.

Liu 등[15]은 RIS를 활용한 MISO(Multiple-Input Single-Output) 다중 사용자 시스템에서 물리계층 비밀키 생성을 연구하였다. 그림 7에 도시된 바와 같이, 송신 측은 다중 안테나를 갖는 기지국(Base Station)으로, 수신 측은 단일 안테나를 갖는 다수의 사용자 단말로 구성되며, RIS는 기지국과 사용자 사이에 배치되어 무선 전파 환경을 능동적으로 제어한다. RIS는 다수의 반사 소자를 통해 신호의 위상 시프트를 조절함으로써 채널 특성을 재구성하고, 이를 비밀키 생성에 유리한 방향으로 조정한다.

무선 채널의 상호성과 무작위성을 기반으로 기지국과 각 사용자 간에 대칭적인 비밀키를 생성하는 절차를 고려하며, 키 생성 이전 단계에서 RIS와 기지국의 파라미터를 사전에 최적화한다는 점이 특징이다. 통계적 채널 상태 정보(Statistical CSI)를 이용하여 RIS의 반사 계수와 기지국의 프리코딩 매트릭스를 공동으로 설계함으로써, 채널의 엔트로피를 증가시키고 다중 사용자 환경에서의 총 비밀키 생성률(SKGR: Sum Key Generation Rate)을 극대화한다.



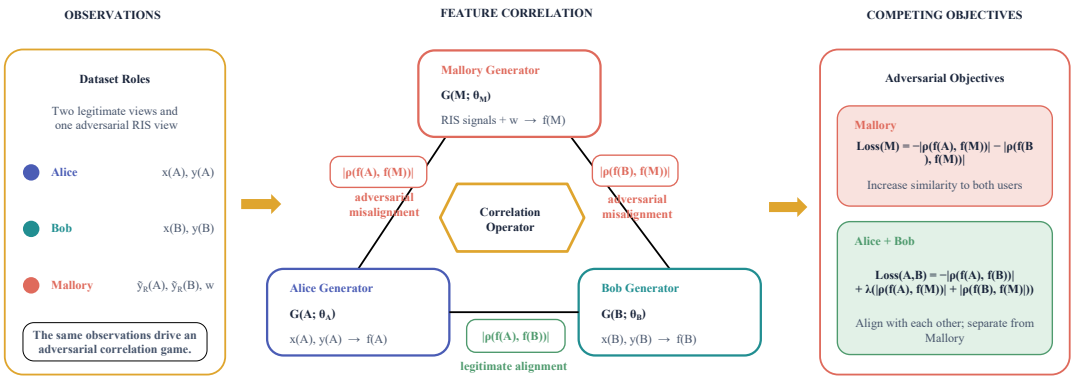
출처 Reprinted from K. Liu et al., "Secret Key Generation for Reconfigurable Intelligent Surface-Assisted MISO Multi-User System," IET Commun., vol. 18, 2024, pp. 1741-1752.

그림 7 RIS-assisted MISO 다중 사용자 시스템을 위한 키 생성 프레임워크

논문은 SKGR에 대한 폐쇄형 표현식을 유도하고, 이를 목적 함수로 하는 공동 최적화 문제를 도출하였다. 해당 문제는 RIS 위상 시프트와 송신 프리코딩이 결합된 비선형 · 비볼록(Non-Convex) 문제이므로 직접적인 해법 도출이 어렵다. 이에 따라 DC-SCA(Difference-of-Convex Successive Convex Approximation) 기반의 반복적 최적화 알고리즘을 제안하여, 기지국과 RIS의 최적 결합 계수를 효율적으로 산출한다. 최적화된 파라미터가 설정된 이후에는 그림 7 하단에 제시된 바와 같이 채널 프로빙, 양자화, 정보 조정, 프라이버시 증폭의 표준적인 물리계층 키 생성 절차를 수행함으로써 다중 사용자 환경에서도 향상된 비밀키 생성 성능을 달성한다.

Wei 등[16]은 정상적인 송수신자(Alice와 Bob) 사이에 개입하는 MITM-RIS(Man-In-The-Middle RIS) 공격을 고려하고, 이를 방어하기 위한 적대적 학습(Adversarial Learning) 기반 물리계층 비밀키 생성 프레임워크를 제안하였다. 일반적으로 정상적인 RIS는 무선 채널의 무작위성을 증대시켜 물리계층 비밀키 생성(PL-SKG: Physical Layer Secret Key Generation)의 성능을 향상시키는 이점을 제공한다. 반면, 악의적인 RIS는 송수신자 간 채널을 능동적으로 조작함으로써 채널 상호성과 무작위성을 훼손하고, 기존의 PL-SKG 기법을 무력화할 수 있는 강력한 중간자 위협으로 작용한다.

그림 8에서 MITM-RIS Eve를 공격자 모델로 정



출처 Author-created conceptual workflow of adversarial feature learning for physical layer secret key generation under a malicious reconfigurable intelligent surface (RIS). The procedural concepts are summarized from [16].

그림 8 Alice-Bob의 공통 특징 생성기를 학습하기 위한 적대적 학습 구조

의하고, Mallory를 Eve가 수행하는 딥러닝 기반 공격을 모사하는 적대적 신경망으로 설정한다. Alice와 Bob은 각각 자신이 관측한 정상적인 양방향 복소 신호(예: I/Q 신호 또는 CSI를 포함하는 신호 표현)를 입력으로 하여, 동일한 구조를 갖는 공통 특징 생성기(Common Feature Generator)를 통해 특징 벡터를 추출한다. 이때 생성되는 공통 특징은 Alice-Bob 간에는 높은 상관성을 유지하지만, MITM-RIS Eve가 관측한 신호로부터는 재구성이 어렵도록 학습된다.

이를 위해 Alice-Bob 간 특징 유사도를 최대화하는 동시에, Alice-Eve(Mallory) 및 Bob-Eve(Mallory) 간 특징 유사도를 최소화하는 적대적 손실 함수를 설계하였다. Mallory 신경망은 Eve가 획득 가능한 정보만을 이용해 Alice-Bob의 특징을 추정하려 시도하며, Alice-Bob의 특징 생성기는 이러한 공격을 방해하는 방향으로 학습된다. 또한, 그림 8에 제시된 공통 특징 생성기는 단순한 블랙박스 신경망이 아니라, xAI(symbolic eXplainable AI) 기법을 통해 수학적으로 해석 가능한 구조로 표현될 수 있음을 보임으로써, 제안된 프레임워크의 물리적 의미와 보안성을 동시에 설명한다.

IV. 결론

본고에서는 무선통신 환경의 급격한 변화와 보안 요구의 고도화에 따라 재조명되고 있는 물리계층 보안기술의 개념과 연구 동향을 종합적으로 고찰하였다. 물리계층 보안기술은 무선 신호가 갖는 고유한 물리적 특성을 활용하여 기존 암호 기반 보안기술이 직면한 키 관리 복잡성, 확장성 한계, 연산 부담, 그리고 양자 컴퓨팅 위협과 같은 문제를 보완할 수 있는 유망한 보안 패러다임으로 자리매김하고 있다.

물리계층 비밀키 생성과 기기 인증을 중심으로, RSS 등 채널과 하드웨어 등의 특징을 체계적으로 분류하고, 환경 적합성 및 보안 관점에서의 특성을 비교 · 분석하였다. 또한, 전통적인 분석 기반 기법의 한계를 극복하기 위한 AI/ML 기반 및 무선 환경을 능동적으로 제어할 수 있는 RIS 기반 보안기술의 최근 연구들을 살펴보았다. 향후 물리계층 보안기술은 상위 계층 암호 기술을 대체하기보다는 상호 보완적인 다계층 보안 구조의 핵심 요소로 발전할 것으로 전망되며, 실제 무선 시스템 적용을 위한 표준화, 성능 검증, 그리고 실환경 기반 평가가 중요한 연구 과제로 남아 있다.

참고문헌

[1] J. Zhang et al., “Experimental Study on Key Generation for Physical Layer Security in Wireless Communications,” IEEE Access, vol. 4, 2016, pp. 4464-4477. doi: 10.1109/ACCESS.2016.2604618

[2] S. Mathur et al., “Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel,” in Proc. ACM Int. Conf. Mobile Comput. Netw., (San Francisco, CA, USA), Sep. 2008, pp. 128-139. doi: 10.1145/1409944.1409960

[3] H. Liu et al., “Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation,” IEEE Trans. Mobile Comput., vol. 13, no. 12, 2014, pp. 2820-2835.

[4] J. Liu and X. Wang, “Physical Layer Authentication Enhancement Using Two-dimensional Channel Quantization,” IEEE Trans. Wireless Commun., vol. 15, no. 6, 2016, pp. 4171-4182.

[5] P. Baracca et al., “Physical Layer Authentication over MIMO Fading Wiretap Channels,” IEEE Trans. Wireless Commun., vol. 11, no. 7, 2012, pp. 2564-2573.

[6] C.D.T. Thai et al., “Secret Group-Key Generation at Physical Layer for Multi-Antenna Mesh Topology,” IEEE Trans. Inf. Forensics Secur., vol. 14, no. 1, 2019, pp. 18-33.

[7] S. Taşcıoğlu et al., “RF Fingerprinting Using Transient-Based Identification Signals at Sampling Rates Close to the Nyquist Limit,” Electronics, vol. 14, no. 1, 2025, 4. doi: 10.3390/electronics14010004

[8] W. Hou et al., “Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets,” IEEE Trans. Commun., vol. 62, no. 5, 2014, pp. 1658-1667.

[9] C. Zhao et al., “A Robust Authentication Scheme Based on Physical-Layer Phase Noise Fingerprint for Emerging Wireless Networks,” Comput. Netw., vol. 128, 2017, pp. 164-171. doi: 10.1016/j.comnet.2017.05.028

[10] P. Hao et al., “Performance Enhancement of I/Q Imbalance Based Wireless Device Authentication Through Collaboration of Multiple Receivers,” in Proc. IEEE Int. Conf. Commun., (Sydney, Australia), June 2014, pp. 939-944.

[11] S. Kojima and S. Sugiura, “User-Independent Randomized Pilot Activation for Secure Key Generation,” IEEE Trans. Wireless Commun., vol. 23, no. 9, 2024, pp. 11624-11635. doi: 10.1109/TWC.2024.3383868

[12] H. Wu et al., “Secret Key Generation With Untrusted Internal Eavesdropper: Token-Based Anti-Eavesdropping,” IEEE Trans. Inf. Forensics Secur., vol. 20, 2025, pp. 2523-2537. doi: 10.1109/TIFS.2025.3542959

[13] F. Ardizzon et al., “A RNN-Based Approach to Physical Layer Authentication in Underwater Acoustic Networks with Mobile Devices,” Comput. Netw., vol. 243, 2024, 110311. doi: 10.1016/j.comnet.2024.110311

[14] A. Elmaghbub and B. Hamdaoui, “HEEDFUL: Leveraging Sequential Transfer Learning for Robust WiFi Device Fingerprinting Amid Hardware Warm-Up Effects,” IEEE Trans. Netw. Serv. Manag., vol. 23, 2026, pp. 123-136. doi: 10.1109/TNSM.2025.3624126

[15] K. Liu et al., “Secret Key Generation for Reconfigurable Intelligent Surface-Assisted MISO Multi-User System,” IET Commun., vol. 18, 2024, pp. 1741-1752.

[16] Z. Wei et al., “Explainable Adversarial Learning Framework on Physical Layer Key Generation Combating Malicious Reconfigurable Intelligent Surface,” IEEE Trans. Wireless Commun., vol. 24, no. 4, 2025, pp. 3529-3545. doi: 10.1109/TWC.2025.3531799