재구성 가능한 지능형 반사 표면(RIS) 기반 물리계층 보안 기법의 비교 연구: 신호 집중, 간섭 제어, 위상 기반 키 활용 방식

정수현, 김현찬, 채대명, 김도은, 정수민*

금오공과대학교 전자공학부/IT융복합공학과
jshyeon2010@naver.com, sumin.jeong@kumoh.ac.kr

Comparative Study of RIS-Based Physical Layer Security Techniques: Beamforming, Interference Control, and Phase-Key Approaches

Suhyeon Jeong, Hyunchan Kim, Daemyeong Chae, Doeun Kim, Sumin Jeong

Kumoh National Institute of Technology.

요 약

무선 통신에서는 상위계층 암호만으로는 채널 도청, 중계 공격, 저지연 키 관리 이슈에 충분히 대응하기 어렵다. 이에 따라 재구성 가능한 지능형 반사 표면(Reconfigurable Intelligent Surface, RIS)을 활용한 물리계층 보안이 상위계층 암호를 보완하는 실용 대안으로 부상하고 있다. 본 논문에서는 재구성 가능한 반사 표면 기반 보안 시스템의 채널 상태 정보 의존성과 도청자 불확실성에 취약한 신호 집중 및 간섭 제어의 한계를 지적하고, 별도 분배 없이 채널 상호성과 RIS 위상 난수성을 활용해 공통 키를 수립하는 위상 기반 키 생성이 차세대 RIS 물리계층 보안의 유력한 방향임을 제시한다.

Ⅰ. 서 론

무선 통신은 시간과 장소에 구애받지 않고 전 세계를 연결하는 데 필수적인 기술로, 다양한 이점을 제공하나 무선 신호의 방송 특성으로 인해 사용자들은 잠재적 공격에 쉽게 노출된다. 이에 따라 통신 보안의 중요성이 한층 부각되었으며, 보안 접근 방식은 크게 네트워크 보안과 물리 계층 보안으로 구분된다 [1]. 그러나 침입 탐지 시스템과 같은 전통적 네트워크 보안 기법은 점점 복잡해지는 네트워크 공격에 점차 효과를 잃어가고 있다 [2]. 이러한 한계를 보완하기 위해 최근 물리 계층 보안(Physical Layer Security, PLS)이 주목받고 있으며, 이는 도청에 대한 정보 보안을 보장하면서도 신뢰성 있는 전송을 유지하는 새로운 연구 분야이다 [3]. 특히, 재구성 가능한 지능형 반사 표면(Reconfigurable Intelligent Surface, RIS)은 저비용 수동 반사 소자 배열을 통해 전파의 크기와 위상을 능동적으로 제어할 수 있어 통신 품질과 보안을 향상하는 잠재력을 지닌다 [4].

이에 따라 본 논문에서는 RIS 기반 물리 계층 보안을 크게 세 가지 방향으로 나누어 소개한다: (i) 합법 사용자 방향으로 전파 에너지를 집중시켜 도청자가 수신하는 신호 세기를 감소시키는 **신호 집중 방식**; (ii) RIS의 위상 조작으로 합법 수신기 쪽의 채널 이득을 증대시키고, 동시에 도청자 쪽에는 의도적 간섭을 강화하여 기밀성을 확보하는 **간섭 제어 방식**; (iii) RIS의 위상 제어값을 암호 키로 매핑/공유하여 합법 사용자만 신호를 복호화하도록 하는 **위상 기반 암호 키 활용 방식**.

Ⅱ. 본론

A. 신호 집중 방식

신호 집중 방식은 RIS의 위상 최적화를 통해 합법 사용자의 유효 채널 이득을 증대시키고 **도청자의 수신 전력을 체계적으로 제거/억제**하여 비밀 전송률을 직접 끌어올리는 물리 계층 보안 기법이다. 구현 측면에서는 다음 네 가지 방식으로 구분할 수 있다 (i) 기지국 - RIS 공동 최적화를 통해 합법 사용자 방향으로 위상 정합을 이루는 **단일 RIS 집중 방식** (불완전한 채널 상태 정보와 도청자 위치 불확실성을 고려한 강건 설계 포함) [5]; (ii) 전/후방을 동시에 제어하는 **STAR-RIS 기반 공간 분할 집중 방식**(에너지/시간 분할 비율 및 위상 패턴 동시 최적화) [6]; (iii) 다중 RIS를 배치하여 경로 다양성과 공간 분산을 이용하는 **협력 집중 방식** (사용자별 가중 합 비밀률 또는 최소 보장 비밀률 기준의 설계) [7]; (iv) 대면적/근접장 조건에서 구면파 전파와 공간-광대역 효과를 반영해 미세 초점을 형성하는 **근접장/홀로그래픽 집중 방식** [8].

보안 관점의 강점은 별도의 키 분배나 인공 잡음 투입 없이 공간 초점 제어만으로 합법 사용자 대비 도청자에게 불리한 채널을 일관되게 조성할 수 있다는 점이다. 다중 사용자/셀-프리 구조나 협력 RIS와 결합해 보안 여유를 추가로 확장할 수 있다는 실용적 확장성도 갖는다. 반면 한계로는 도청자 위치/채널 모델의 불확실성에 대한 성능 민감도(최적화 해가 쉽게 취약해질 수 있음), 위상 양자화/보정 오차/반사 단위 간 편차 등 하드웨어 비이상성으로 인한 초점 붕괴, 근접장/대규모 표면에서의 고차 비선형 제약으로 인해 생기는 계산 복잡도와 온라인 재구성 지연 문제가 존재한다. 따라서 실제 시스템 적용을 위해서는 분포/세트 기반의 강건 설계, 위상 오차를 흡수하는 결함인지 위상 패턴, 사용자·도청자 군집을 고려한 다목적(비밀률-전력-지연) 공동 최적화, 그리고 빠른 재구성을 위한 경량 근사·학습형 제어 전략 등이 필수적이다.

B. 간섭 제어 방식

간섭 제어 방식은 RIS의 위상 패턴을 설계하여 합법 사용자 채널의 이득은 보존하면서 **도청자 채널에 선택적 간섭을 유발/강화**함으로써 비밀 전송률을 높이는 물리 계층 보안 기법이다. 현 측면에서는 다음 네 가지 방식으로 구분할 수 있다: (i) 기지국 - RIS 공동 최적화를 통해 합법 사용자 신호는 정합시키고 도청자 널 공간 또는 특정 차원에 **인공 잡음을 주입하는 설계 방식** [9], (ii) 다중 사용자 환경에서 송신 빔/RIS 위상/인공 잡음 전력 분배를 동시에 조정해 **가중 합 비밀률을 극대화하는 설계 방식** [10], (iii) 통합 감지-통신(Integrated Sensing and Communications, ISAC) 시나리오에서 감지 신호를 도청자에게 간섭으로 활용하고 합법 사용자에 대한 **간섭 누설을 억제하는 설계 방식** [11], (iv) 도청자 위치/채널 불확실성을 고려한 강건(Robust, 분포/세트 기반) **최적화 및 강화학습 기반 적응 제어 방식** [12].

이 접근의 강점은 별도의 키 분배 없이 공간적 간섭 조형만으로 도청자 신호 대 잡음비(SNR)/신호 대 잡음 및 간섭비(SINR)를 체계적으로 열화시킬 수 있다는 점이며, 마찬가지로 다중 사용자/셀-프리 구조로 확장이 용이하다는 실용성이 있다. 반면, 이 접근 방법은 간섭 누설로 인한 합법 사용자 성능 저하 위험, 도청자 CSI 불확실성에 대한 민감도, 위상 양자화/보정 오차 등 하드웨어 비이상성의 영향, 그리고 대규모 표면/다목적(비밀률 - 전력 - 지연) 공최적화에서의 높은 계산 복잡도와 온라인 재구성 지연이 존재한다는 한계를 가진다.

C.위상 기반 암호 키 활용 방식

위상 기반 암호키 활용 방식은 RIS의 위상 제어값이나 채널 무작위성을 직접 비밀키로 변환해 사용하는 물리계층 보안 기법이다. 이 방식은 합법

송수신자가 공유하는 채널 상호성(channel reciprocity)과 RIS 반사 위상의 난수성을 기반으로 공통 키를 생성하고, 해당 키를 알고 있는 사용자만 신호를 복원할 수 있도록 설계된다. 구현 방법은 크게 다음과 같다: (i) RIS의 위상 패턴을 슬롯마다 무작위로 변화시켜 송수신자가 동시에 동일한 키를 도출, 도청자에겐 키가 불확실하게 보이도록 하는 RIS 위상 시프트 난수화 기반 **원타임 패드(OTP) 키 생성 방식** [13]; (ii) 도청자가 합법 사용자와 유사한 채널을 가질 때 키 생성 속도가 저하되는 문제를 해결하기 위해 합법 쌍의 채널 추정값을 RIS 동적 제어와 결합하여 비밀키 생성률을 향상시키는 **CSI 기반 RIS 동적 제어를 통한 키 생성 방식** [14]; (iii) 다중 경로와 공간 상관도를 RIS 배치와 제어로 조정해 합법 채널의 무작위성을 증폭시킴으로써 키 생성 성능을 강화하는 **공간 상관 채널 환경에서 RIS 활용 방식** [15].

이 접근 방법의 장점은 별도의 키 분배 절차 없이 채널 자체를 이용해 보안성을 확보할 수 있고, 도청자에 대한 강인성이 높으며 추가 전력 소모 없이 에너지 효율적으로 동작한다는 점이다. 반면, 한계로는 합법 사용자 간 채널 상호성이 완벽하지 않을 경우 키 일관성이 떨어질 수 있으며, 공간 상관도가 높거나 도청자가 합법 사용자와 유사한 채널을 가질 경우 키 생성 성능이 저하될 수 있다.

D. 비교 분석

최종적으로 신호 집중 방식은 RIS 위상을 정밀히 조정하여 합법 사용자에게 신호를 모으고 도청자 방향의 누설을 약화시키는 접근으로, 구현이 비교적 단순하고 즉각적인 비밀 전송률 향상 효과가 있으나 도청자 위치/채널 정보에 대한 정확한 추정이 요구된다는 한계가 있다. 간섭 제어 방식은 인공 잡음이나 위상 패턴을 통해 도청자에게 선택적 간섭을 가함으로써 보안을 강화하지만, 합법 사용자 채널까지 간섭의 영향을 받을 수 있고, CSI 불확실성에 따라 성능 저하가 크다는 문제가 있다. 반면, 위상 기반 암호키 활용 방식은 RIS 위상 무작위성과 채널 상호성을 이용해 합법 사용자 간에 공통 키를 동적으로 생성함으로써 별도의 키 분배 절차 없이 안전성을 확보하고, 도청자가 동일한 키를 추출하기 어렵도록 설계되어 환경 변화와 하드웨어 제약에도 강인하다. 따라서 RIS 물리계층 보안의 세 가지 대표적 접근 중, 위상 기반 암호 키 활용 방식이 차세대 무선 네트워크에서 가장 유력한 발전 방향으로 평가된다.

Ⅲ. 결론

본 논문은 RIS 기반 물리계층 보안을 신호 집중, 간섭 제어, 위상 기반 암호 키 활용의 세 축으로 정리하고, 각각의 구현 범주와 한계를 체계적으로 검토하였다. 신호 집중은 직관적이며 즉시적인 비밀 전송률 향상을 제공하지만 도청자 정보/하드웨어 오차에 민감하고, 간섭 제어는 선택적 교란으로 보안을 강화하되 합법 사용자 품질 저하와 불확실성 대응이 과제로 남는다. 이에 비해 위상 기반 암호 키 활용은 채널 상호성과 RIS 위상 난수성을 이용해 상위 계층 키 분배 없이 공통 키를 동시 생성함으로써 도청자에 강인한 보안성을 제공하고, 에너지/프로토콜 측면에서도 실용성이 높다. 따라서 차세대 RIS 물리계층 보안의 핵심 방향은 위상 기반 암호 키 활용에 있으며, 향후 연구는 도청자 불확실성 하의 강건 키 생성, 공간 상관·근접장 효과를 반영한 위상 제어, 그리고 저복잡 실시간 제어·검증 프레임워크로의 이행에 초점을 맞출 필요가 있다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신 기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임 (IITP-2025-RS-2020-II201612)

참 고 문 헌

[1] L. Sun and Q. Du, "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions," in Entropy(Basel), vol. 20, no. 10, pp. 1-21, 2018, doi: 10.3390/e20100730.

[2] D. Zhao, G. Ji, Y. Zhang, X. Han and S. Zeng, "A Network Security Situation Prediction Method Based on SSA-GResNeSt," in IEEE Transactions on Network and Service Management, vol. 21, no. 3, pp. 3498-3510, June 2024, doi: 10.1109/TNSM.2024.3373663

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014, doi: 10.1109/SURV.2014.012314.00178.

[4] M. H. Khoshafa et al., "RIS-Assisted Physical Layer Security in Emerging RF and Optical Wireless Communications Systems: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 27, no. 4, pp. 2156-2203, Aug. 2025

[5] X. Yu, D. Xu, Y. Sun, D. W. K. Ng and R. Schober, "Robust and Secure Wireless Communications via Intelligent Reflecting Surfaces," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 11, pp. 2637-2652, Nov. 2020, doi: 10.1109/JSAC.2020.3007043.

[6] T. Zhou, K. Xu, G. Hu, X. Xia, W. Xie and C. Li, "Robust Beamforming Design for STAR-RIS-Assisted Anti-Jamming and Secure Transmission," in IEEE Transactions on Green Communications and Networking, vol. 8, no. 1, pp. 345-361, March 2024, doi: 10.1109/TGCN.2023.3329127.

[7] Y. Xiu, J. Zhao, C. Yuen, Z. Zhang and G. Gui, "Secure Beamforming for Multiple Intelligent Reflecting Surfaces Aided mmWave Systems," in IEEE Communications Letters, vol. 25, no. 2, pp. 417-421, Feb. 2021, doi: 10.1109/LCOMM.2020.3028135.

[8] Xu, Yiming, Jinshuo Liu, Xiaoguang Wu, Tianwen Guo, and Huadong Peng, "Reconfigurable Holographic Surface-Assisted Wireless Secrecy Communication System," in Electronics, vol. 13, no. 7:1359, 2024, doi.org/10.3390/electronics13071359

[9] X. Lu, W. Yang, X. Guan, Q. Wu and Y. Cai, "Robust and Secure Beamforming for Intelligent Reflecting Surface Aided mmWave MISO Systems," in IEEE Wireless Communications Letters, vol. 9, no. 12, pp. 2068-2072, Dec. 2020, doi: 10.1109/LWC.2020.3012664.

[10] B. Wu, and Y. Wu, "Weighted Secrecy Sum Rate Optimization for Simultaneously Transmitting and Reflecting Reconfigurable Intelligent Surface-Assisted Multiple-Input Single-Output Systems," in Applied Sciences, vol. 14, no. 17:7932, 2024, doi.org/10.3390/app14177932.

[11] J. Chen, K. Wu, J. Niu, and Y. Li, "Joint Active and Passive Beamforming in RIS-Assisted Secure ISAC Systems," in Sensors, vol. 24, no. 1:289, 2024, doi.org/10.3390/s24010289

[12] S. Hong, C. Pan, H. Ren, K. Wang, A. Nallanathan and H. Li, "Robust Transmission Design for Intelligent Reflecting Surface Aided Secure Communications," in 2020 IEEE Global Communications Conference (GLOBECOM), Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322565.

[13] Z. Ji et al., "Random Shifting Intelligent Reflecting Surface for OTP Encrypted Data Transmission," in IEEE Wireless Communications Letters, vol. 10, no. 6, pp. 1192-1196, June 2021, doi: 10.1109/LWC.2021.3061549.

[14] N. Gao, Y. Yao, S. Jin, C. Li and M. Matthaiou, "Integrated Communications and Security: RIS-Assisted Simultaneous Transmission and Generation of Secret Keys," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 7573-7587, 2024, doi: 10.1109/TIFS.2024.3436885.

[15] L. Hu, G. Li, X. Qian, A. Hu and D. W. K. Ng, "Reconfigurable Intelligent Surface-Assisted Secret Key Generation in Spatially Correlated Channels," in IEEE Transactions on Wireless Communications, vol. 23, no. 3, pp. 2153-2166, March 2024, doi: 10.1109/TWC.2023.3296076.