시간 선택적 페이딩 채널에서의 DQN 기반 물리 계층 보안 향상

김 규 림, 이 상 철, 김 동 진, 채 승 호*

한국공학대학교

starsirius49@tukorea.ac.kr, *shchae@tukorea.ac.kr

DQN based Physical Layer Security Enhancement in Time-Selective Fading Channels

Gyulim Kim, Sangcheol Lee, Dongjin Kim, Seong Ho Chae*

Tech University of Korea

요 약

본 연구는 시간 상관도가 동적으로 변하는 환경에 대해, 보안 전송률 최대화를 위한 DQN(Deep Q-Network) 기반 적응적 코드워드 데이터율 및 보안 데이터율 선택 방법을 제안하고, 성능을 비교 분석한다.

Ⅰ. 서 론

정적(static) 페이딩 채널 환경에 대해 Alamouti 시공간 블록 부호(Space-time block code)가 처음으로 제안된 이래로, 다양한 직교/준직교 시공간 블록 부호들이 제안되었다[1]. 최근, 시간 선택적 페이딩 채널 환경에서 Alamouti 시공간 블록 부호 전송시 얻을 수 있는 보안 전송률에 대한 연구가 수행되었다[2]. 수신기와 도청기에 대한 LML(Linear Maximum Likelihood)과 ZF(Zero-forcing) 복호 방법의 조합에 대해, 완전탐색(exhaustive searching) 방법으로 찾은 최적의 코드워드 및 보안 데이터율이 보안 전송률 최대화 시킬 수 있음을 보였다. 하지만, 이러한 완전 탐색 방법은 상당한 시간 소요를 발생시킴에 따라, 채널의 시간 상관도(time correlation)가 동적(dynamic)으로 바뀌는 실제 환경에 적용하기에는 제한적이다. 따라서, 본 논문에서는 시간 상관도가 동적으로 변하는 환경에 대해, 보안 전송률 최대화를 위한 DQN(Deep Q-Network) 기반 적응적 코드워드 데이터율 및 보안 데이터율 선택 방법을 제안하고, 성능을 비교 분석한다.

Ⅱ. 시스템 모델

송신기(Alice)는 2개의 안테나를 가지며, 수신기(Bob)와 도청기(Eve)는 각기 1개의 안테나를 가지는 환경을 고려한다. 송신기는 보안 데이터율 R_S를 기반으로 임의의 두 데이터율 R_T와 R_E를 설정함으로써 Wyner 코드북을 생성한다. 이때, $R_S = R_T - R_E$를 만족한다. 송신기는 Alamouti 시공간 블록 부호를 활용하여 수신기에게 보안 메시지를 전송하고, 도청기는 이를 도청한다. 실시간 변화하는 시간 상관도의 문제를 MDP(Markov Decision Process)로 변환하고, DQN 알고리즘을 활용하여 최적화한다.

- (상태 집합) Wyner 코드북의 R_T, R_E의 값이며, 다음과 같이 정의한다.

$$S = \{s_1, s_2, \dots, s_n\},\ s_i \in \{0 \le R_T, R_E \le 8\},\ \forall i. \quad (1)$$

- (행동 집합) 에이전트(송신자)는 각 R_T, R_E의 값을 제어함에 따라, 행동 집합을 다음과 같이 정의한다.

$$A = \{a_1, a_2, \dots, a_n\}, a_i \in \{\triangle R_T, -\triangle R_T, \triangle R_E, -\triangle R_E\}\ \forall i. \quad (2)$$

- (보상) 보상(reward)을 시간 상관도(ρ_B, ρ_E)와 각 에피소드에서의 상태인 R_T, R_E를 통해 산출되는 보안 전송률의 함수로 다음과 같이 정의한다.

$$R = \begin{cases} r & (\text{if } R_T > R_E) \\ 10r & (\text{if } R_T < R_E,\ r < 0), \end{cases} \quad (3)$$

여기서, $r = R_S(1 - \Pr[E_{co}])(1 - \Pr[E_{so}])$, E_{co}는 연결 아웃티지 발생 사건, E_{so}는 보안 아웃티지 발생 사건을 의미한다[2].

Ⅲ. 결과 분석 및 결론

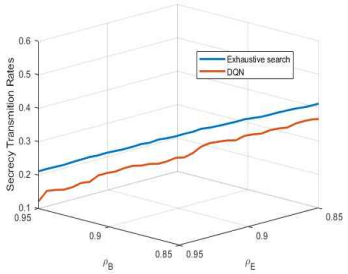

그림 1 . 강화학습 모델과 완전 탐색의 Secrecy Transmission Rates 비교

그림 1은 시간 선택적 페이딩 채널에서 시간 상관도가 변할 때, 완전 탐색 성능과 강화학습 모델의 보안 전송률 성능을 보여준다. 레일레이 페이딩 채널에서 완전 탐색은 $0 \le R_E, R_T \le 8\,(bps/Hz)$에서 적용되며, 시간 상관도는 다음의 범위 $0.85 \le \rho_B, \rho_E \le 0.95$의 무작위 값을 입력하여 학습을 진행하였다. 완전 탐색 성능 대비 DQN 강화학습 모델은 83%의 성능을 보여준다. 완전 탐색은 약 25초의 계산 시간이 소요된 반면, 학습이 완료된 모델은 약 0.3초의 소요 시간이 발생하였다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업(IITP-2023-RS-2022-00156326)과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행되었음 (No. NRF-2021R1F1A1050633)

참 고 문 헌

[1] S. H. Chae, I. Bang, and H. Lee, “Physical layer security of QSTBC with power scaling in MIMO wiretap channels,“ *IEEE Trans. Veh. Tech.*, vol. 69. no. 5, pp. 5647-5651, May 2020.

[2] D. Kim, G. Kwon, H. Lee, and S. H. Chae, ''On the Achievable Secrecy Transmission Rates by Alamouti Space‐Time Block Coding in Time-Selective Fading Channels,'' IET Electronics Letters, vol. 58, no. 17, pp.672-674, Aug. 2022.