International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Physical Layer Security Enhancement Assisted by Intelligent Reflecting Surface Based on Deep Q-Network

Zhiling Zhou
School of Management Science and Engineering, Anhui University of Finance and Economics
Email address: 743777385@qq.com

***Abstract*—*With the rapid development of wireless communication technologies, particularly the evolution of 5G and the anticipation of 6G systems, the importance of Physical Layer Security (PLS) as a crucial technology for ensuring wireless communication security has become increasingly significant. This paper introduces an Intelligent Reflecting Surface (IRS)-assisted PLS enhancement scheme based on Deep Q-Network (DQN). The objective of this scheme is to optimize wireless channel conditions by dynamically adjusting IRS parameters, ultimately enhancing both the system's security and communication efficiency. The paper commences by outlining the fundamental workings of IRS and its vast potential in bolstering PLS. Subsequently, it delves into the intricate details of the IRS optimization strategy rooted in DQN. Lastly, the effectiveness of this proposed scheme is substantiated through rigorous simulation experiments.*

***Keywords*—*Sixth – Generation, Physical Layer Security, Deep Q - Network, Intelligent Reflecting Surface*.

I. INTRODUCTION

In the field of wireless communication, Physical Layer Security (PLS), as a technology that utilizes the inherent characteristics of wireless channels to achieve secure transmission, has received widespread attention in recent years. However, traditional PLS methods often struggle to achieve ideal protection effects when confronted with complex and dynamic wireless environments. Intelligent Reflecting Surface (IRS), an emerging programmable electromagnetic surface, is capable of dynamically reconfiguring the wireless propagation environment through intelligent control of the reflection phases and amplitudes of its surface elements, providing a novel solution for PLS.

Amidst the rapid advancements in wireless communication technologies, Physical Layer Security (PLS), as an innovative security strategy, is gradually emerging as a critical cornerstone for ensuring the security of data transmission. This technology leverages the natural characteristics of wireless channels, such as noise, interference, and fading, to achieve secure transmission mechanisms without the need for complex key exchanges, by designing specific signal waveforms and processing methods. However, as wireless communication environments become increasingly complex and dynamic, traditional PLS methods face unprecedented challenges, particularly when confronted with dynamically changing channel conditions, densely deployed network architectures, and increasingly sophisticated eavesdropping techniques, rendering their protection effects often suboptimal.

Against this backdrop, IRS, as a revolutionary technological breakthrough, offers a new solution path for PLS. IRS is a programmable electromagnetic surface composed of numerous low-cost, passive reflecting elements that can dynamically reconfigure the wireless propagation environment through intelligent control of the reflection phases and amplitudes of each element. This high degree of flexibility and customizability enables IRS to precisely adjust signal propagation paths and intensities for different communication scenarios and security requirements, thereby significantly enhancing the security of communication systems at the physical layer.

Specifically, through fine-grained control of its surface elements, IRS can achieve security enhancements in several aspects: In communication links between legitimate users and base stations, IRS can enhance the signal strength at the legitimate receiver through coordinated reflection, while simultaneously suppressing the reception by eavesdroppers. This asymmetric signal enhancement mechanism can effectively increase the system's secure rate and reduce the risk of information leakage. IRS can be integrated with covert communication techniques to make legitimate communication links difficult to detect by eavesdroppers by altering the transmission characteristics and paths of signals. This covertness not only enhances the confidentiality of communication but also makes it difficult for eavesdroppers to locate the position and communication behavior of legitimate users. In the face of complex and dynamic wireless environments, IRS can adjust its reflection characteristics in real-time to adapt to changes in channel conditions. This dynamic reconfiguration capability enables IRS to exhibit greater robustness and adaptability when confronted with adverse factors such as sudden interference and channel fading.

As an emerging programmable electromagnetic surface technology, Intelligent Reflecting Surface (IRS) provides a novel solution for physical layer security in the field of wireless communications. By knowing how to control the reflectivity and power of surface elements, IRS can reshape the wireless communication environment and improve the security and reliability of communication systems. With continuous technological advancements and improvements, IRS is expected to play an increasingly important role in

Zhiling Zhou, "Physical Layer Security Enhancement Assisted by Intelligent Reflecting Surface Based on Deep Q-Network," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 3, pp. 21-24, 2024.

future wireless communication networks, emerging as one of the key technologies for ensuring secure data transmission.

II. Theoretical Basis and Related Work

A. Deep Q-Network

Deep Q-Network (DQN), a milestone achievement in the field of artificial intelligence, ingeniously combines the powerful representation capabilities of deep learning with the decision-making optimization mechanisms of reinforcement learning, paving a new path for tackling complex, high-dimensional decision-making problems. n traditional Q-learning algorithms, facing vast state and action spaces, directly storing and updating the Q-value table (i.e., the value estimates of state-action pairs) becomes extremely unrealistic, a phenomenon known as the "curse of dimensionality." DQN fundamentally addresses this issue by introducing a neural network as an approximator of the Q-function, enabling efficient estimation and generalization of Q-values.

Specifically, DQN employs two core strategies to optimize its learning process: Experience Replay and Target Network. The Experience Replay mechanism maintains a Replay Buffer to store state transition samples (including the current state, taken action, obtained reward, and next state) encountered by the agent during exploration. During training, a small group of samples is randomly sampled from the replicated pool to update the neural network. This approach breaks the physical bond between students and increases the stability and efficiency of learning.

Additionally, DQN incorporates the ε-greedy Policy for action selection, where the agent randomly selects actions with a certain probability ε during the early stages of training to thoroughly explore the environment; as training progresses, ε gradually decreases, and the agent becomes more inclined to select actions with the highest estimated value to exploit existing knowledge, thereby achieving a balance between exploration and exploitation. Through its unique algorithm design and powerful learning capabilities, DQN not only solves the curse of dimensionality in high-dimensional spaces inherent in traditional Q-learning but also provides new avenues for intelligent decision-making in complex environments, serving as a crucial driving force in the advancement of artificial intelligence technology.

B. Intelligent Reflecting Surface.

Intelligent Reflecting Surface (IRS), as a cutting-edge electromagnetic manipulation technology, revolves around its meticulously designed two-dimensional artificial electromagnetic surface structure, comprising thousands of tiny, low-cost, and passive reflecting elements densely arranged. ach reflecting element possesses high degrees of independence and programmability, enabling precise control over the reflection phase and (in some designs) reflection amplitude of incident electromagnetic waves. This characteristic allows IRS to act as an intelligent mirror, offering unprecedented flexibility in manipulating the propagation paths of wireless signals.

In wireless communication systems, the propagation of wireless signals is often affected by complex environmental factors, such as multipath effects and shadow fading, which not only degrade the signal quality but also potentially create opportunities for eavesdropping by unauthorized listeners. Intelligent Reflecting Surfaces (IRS) can dynamically adjust the states of their surface reflective elements, enabling them to actively direct the propagation of electromagnetic waves along specific paths, effectively enhancing the signal strength at the intended receiver (e.g., legitimate user devices), while simultaneously attenuating or redirecting signals that may leak to unauthorized receivers (e.g., eavesdroppers), thereby establishing an invisible security barrier at the physical layer.

With their unique capabilities in electromagnetic manipulation and flexible configuration, IRSs offer new technical dimensions and solutions for enhancing physical layer security. As research continues to deepen and technologies mature, IRSs are poised to play an increasingly important role in future wireless communication systems, contributing to the development of secure, efficient, and reliable communication environments.

III. System Model and Problem Definition

A. System Model

This paper considers a wireless communication system comprising a Base Station (BS), a Legitimate User (LU), and an Eavesdropper (Eav). The BS transmits confidential information to the LU via an Intelligent Reflecting Surface (IRS), while the Eav attempts to intercept this information. The BS sends confidential information to the LU through the IRS, while the Eav endeavors to intercept this information. To ensure communication security, we employ Deep Q-Network (DQN) to optimize the configuration parameters of the IRS, aiming to maximize the received signal quality at the LU while minimizing that at the Eav.

B. Problem Definition.

The goal of this document is to increase the security rate of the user directly by optimizing the IRS configuration parameters while meeting certain power and interference constraints. This problem can be formulated as a Markov Decision Process (MDP), where the configuration parameters of the IRS serve as the action space, and the secure rate of the legitimate user acts as the reward function.

IV. Design of the Deep Q-Network

The DQN architecture comprises two integral components: a Deep Neural Network (DNN) and the Q-learning algorithm. The DNN serves as an approximator for the Q-value function, enabling the system to estimate the expected reward for a given state s and action a. Meanwhile, the Q-learning algorithm directs the training process of the DNN by iteratively updating the Q-value table, thereby optimizing the configuration parameters of the Intelligent Reflecting Surface (IRS).

A. State Space Definition

The state space is meticulously defined to encapsulate the current state information of the wireless channel. This includes the channel gains between the Base Station (BS), IRS, Legitimate User (LU), and Eavesdropper (Eav), as well as the current reflection phase configuration of the IRS. This comprehensive state representation ensures that the DQN can make informed decisions based on the current channel conditions.

B. Action Space Specification

The action space is precisely defined as the set of possible reflection phase configurations that the IRS can adopt. Each action within this space corresponds to a unique IRS configuration scheme, allowing the DQN to explore and exploit different IRS settings to maximize the system's performance.

C. Reward Function Design

The reward function is intricately crafted to align with the objective of enhancing the system's security rate. Specifically, it is designed as a function of the difference between the received signal quality at the LU and that at the Eav. When the system's security rate improves, indicating a stronger signal for the LU and a weaker signal for the Eav, the reward value increases. Conversely, any degradation in the security rate leads to a decrease in the reward value, thereby guiding the DQN towards configurations that maximize the system's security.

D. Algorithm Execution Flow

Step 1: Initialization

Commence by initializing the key components of the DQN framework. Define the network architecture of the Deep Neural Network (DNN), set the learning rate, the discount factor, and any other relevant hyperparameters. Additionally, initialize the Q-value table, which will serve as the basis for learning and decision-making.

Step 2: Data Acquisition

At each time step, the algorithm observes the current state of the wireless environment, encompassing the channel conditions and IRS configuration. Based on this state, an action (IRS configuration) is selected from the action space, typically utilizing an exploration-exploitation strategy such as ε-greedy. The execution of this action results in a reward signal and the transition to a new state. These observations (state, action, reward, next state) are recorded for subsequent use.

Step 3: Experience Replay

To enhance the efficiency and stability of the learning process, implement experience replay. Gather the recorded observations into a replay memory, also known as an experience pool. During training, randomly sample a batch of experiences from this pool. This mechanism breaks the temporal correlations in the data and provides a more diversified set of experiences for the DNN to learn from.

Step 4: Network Training

Leverage the sampled experiences to train the DNN. Specifically, utilize the Q-learning algorithm to update the DNN's weights. This involves computing the target Q-values for each experience, based on the current Q-value table and the observed rewards and next states. Next, optimize the DNN parameters to minimize the difference between the predicted Q values (DNN output) and the actual Q values. This step aims to refine the DNN's ability to approximate the Q-value function accurately.

Step 5: Policy Update

After each training iteration, update the Q-value table based on the improved DNN. The updated Q-values reflect the newfound knowledge about the optimal actions in various states. Consequently, adjust the IRS configuration parameters according to the current estimates of the optimal policy, derived from the Q-value table.

Step 6: Iteration and Convergence

Repeat steps 2 through 5 iteratively, continually acquiring new data, training the DNN, and updating the policy. Continue this process until a predetermined number of training epochs have been completed or a convergence criterion (e.g., stabilization of the reward signal) is met. Through this iterative process, the DQN gradually learns to optimize the IRS configuration for maximizing the system's security rate.

E. Simulation Experiments and Result Analysis

To validate the effectiveness of the proposed DQN-based IRS-assisted physical layer security enhancement scheme, we conducted simulation experiments using MATLAB. The experimental results demonstrate that, compared to traditional physical layer security methods without IRS, our scheme is able to significantly improve the system's security rate and reduce the security outage probability. Specifically, under the same channel conditions, our scheme achieves higher LU received signal quality and lower Eav received signal quality, thereby enhancing the security of the system.

V. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This paper introduces an innovative approach for enhancing physical layer security utilizing Deep Q-Network (DQN) in conjunction with Intelligent Reflecting Surfaces (IRS). By dynamically adjusting the IRS configuration parameters, our scheme meticulously optimizes the wireless channel conditions, thereby bolstering both the security and communication efficiency of the system. This meticulous optimization process ensures that the transmitted signals are not only protected from eavesdropping but also delivered with minimal distortion and delay.

The simulation experiments conducted to validate this concept have yielded remarkable results. Compared to conventional physical layer security methods, our proposed scheme demonstrates a significant improvement in system security rates, ensuring that confidential information is transmitted securely and efficiently. Additionally, it effectively reduces the security outage probability, mitigating the risk of communication disruption caused by external interference or eavesdropping attempts.

Looking ahead, our future endeavors will be directed towards refining the DQN algorithm to achieve even higher levels of optimization and adaptability. We aim to explore novel training strategies and network architectures that can better harness the potential of DQN in dynamically adjusting IRS parameters. Furthermore, we envision extending the application scope of IRS by investigating its integration with other cutting-edge technologies, such as massive Multiple-Input Multiple-Output (MIMO) systems and terahertz communications.

The combination of IRS with massive MIMO, for instance, could potentially unlock new dimensions of beamforming and spatial multiplexing, significantly enhancing spectral efficiency and reducing interference. On the other hand, integrating IRS into terahertz communication systems could overcome the challenges posed by severe path loss and molecular absorption at these frequencies, enabling the realization of ultra-high-speed and secure wireless links.

In conclusion, our work represents a significant step forward in the realm of physical layer security, demonstrating the potential of IRS-assisted systems in enhancing the overall performance of wireless communication networks. As we continue to refine our approach and explore new avenues of integration, we anticipate that the benefits of this technology will become even more pronounced, paving the way for more secure, efficient, and reliable wireless communication in the future.

REFERENCES

[1] DI RENZO M, NTONTIN K, SONG Jian, et al. Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison[J]. IEEE Open Journal of the Communications Society, 2020, 1: 798–807.

[2] BJÖRNSON E, ÖZDOGAN Ö, and LARSSON E G. Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying[J]. IEEE Wireless Communications Letters, 2020, 9(2): 244–248.

[3] Amri M.M. Recent Trends in the Reconfigurable Intelligent Surfaces (RIS): Active RIS to Brain-controlled RIS[C]. 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Solo, Indonesia, 2022: 299-304.

[4] YU XH, XUD F, SCHOBER R Enabling secure wireless communications via intelligent reflecting surfaces[C]// Proceedings of 2019 IEEE Global Communications Conference. Piscataway: IEEE Press,2019:1-6.

[5] HUANG C W, ZAPPONE A, ALEXANDROPOULOS G C, et al. Reconfigurable intelligent surfaces for energy efficiency in wireless communication[J]. IEEE Transactions on Wireless Communications,2019,18(8):4157-4170.