The rapid advancement of wireless communication technologies has led to the development of sophisticated techniques to enhance communication performance and security, with Reconfigurable Intelligent Surfaces (RIS) emerging as a promising technology for future wireless communication systems (Ayub, 2021). RIS can configure the wireless environment by tuning the phase shifts of reflecting elements, and efficient signal processing techniques are crucial for its performance benefits (Pan, 2021). Recent advances in metamaterials have further enhanced RIS's potential for 6G wireless communications, with a focus on its working principles, hardware structures, and potential benefits (Zhang, 2023).

In parallel, ensuring secure communication in the presence of eavesdroppers has become a critical concern. Secrecy rate, which measures the difference between the capacity of the legitimate user's channel and that of the eavesdropper's channel, is a key metric in evaluating the security of wireless communication systems (Li, 2020) . Traditional methods to maximize secrecy rate often involve complex optimization problems that are difficult to solve in real-time.

Recent advancements in machine learning, particularly Deep Reinforcement Learning (DRL), have shown great potential in solving complex optimization problems in dynamic and uncertain environments. DRL algorithms can learn and adapt to varying conditions, making them suitable for optimizing the secrecy rate in RIS-aided communication networks Nguyen (2023).

This paper proposes a novel DRL-based framework for maximizing the secrecy rate in RIS-assisted communication networks. The main contributions of this paper are organized as follows:

System Model and Problem Formulation: We present a detailed system model for the RIS-assisted communication network and formulate the problem of maximizing the secrecy rate.

SD3-based Framework: We introduce a robust DRL-based optimization framework, leveraging the Soft Actor-Critic (SAC) algorithm, to address the secrecy rate maximization problem.

Performance Evaluation: We conduct extensive simulations to evaluate the performance of the proposed framework and demonstrate its effectiveness in enhancing the secrecy rate.