Cybersecurity Impact of AI Optimization in B5G Networks

Alex Pierron[†], Michel Barbeau[‡], Jose Rubio-Hernan[†], Luca De Cicco[⋆], Joaquin Garcia-Alfaro[†]

[†]SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France
[‡]Carleton University, School of Computer Science, Ottawa, Canada
[⋆]Politecnico di Bari, Dipartimento di Ingegneria Elettrica e dell'Informazione, Bari, Italy

***Abstract*—This paper delves into the application of Deep Reinforcement Learning (DRL) for Reconfigurable Intelligent Surfaces (RISs) to enhance wireless networks capabilities. RIS uses beamforming to reflect signals and is instrumental in improving network efficiency and service quality in B5G and 6G networks. Although DRL provides real-time adaptability, it also may introduce security risks due to the lack of explainability in deep learning models. Our current research focuses on developing a simulation environment to rigorously test the robustness of DRL models against attacks such as eavesdropping. By analyzing these vulnerabilities, we aim to develop more resilient DRL models and effective mitigation strategies. This work is foundational for future research on the security of DRL-driven RIS, paving the way for more capable, secure, and robust communication networks.**

***Index Terms*—Reconfigurable Intelligent Surface, Deep Reinforcement Learning, Cybersecurity, B5G & 6G networks**

I. Introduction

Reconfigurable Intelligent Surface (RIS) is a new technology aimed at improving wireless communications both in terms of capacity and coverage [10]. These innovative devices are composed of arrays of low-cost reconfigurable elements that can dynamically alter the wireless propagation environment by reflecting signals in a controlled and precise manner. Using advanced beamforming techniques, RIS can significantly improve signal precision, thus improving overall network efficiency and reliability [6]. This capability makes RIS a pivotal component in the ongoing evolution toward B5G (Beyond 5G) and 6G networks, where the demand for higher data rates, lower latency and seamless connectivity is ever increasing. Figure 1 illustrates how RISs will be integrated into the B5G and 6G infrastructure.

RIS technology offers a multitude of advantages that address the challenges facing current wireless networks [6]. By optimizing signal paths and mitigating interference, RIS can substantially reduce energy consumption. Moreover, their ability to adapt to dynamic network conditions in real time allows to provide superior quality of service, even in complex and congested environments [6]. This adaptability is particularly crucial as the number of connected devices continues to grow exponentially, driven by the Internet of Things (IoT) and other emerging technologies.

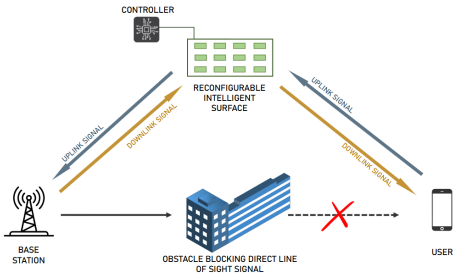

Fig. 1: General usage framework for RIS in B5G and 6G networks

II. The Role of Reinforcement Learning in RIS

Recent advancements in Artificial Intelligence (AI), particularly in Reinforcement Learning (RL) [13], have shown great potential in optimizing RIS performance [7]. RL models, including Deep Reinforcement Learning (DRL), are highly effective in adapting to dynamic network conditions in real time by continuously interacting with the environment to learn optimal policies. This adaptability is crucial for managing the complex and time-varying nature of wireless networks, where signal paths and interference patterns change unpredictably. By utilizing DRL techniques and advanced architectures such as Deep Deterministic Policy Gradient (DDPG) [9], Twin Delayed DDPG (TD3) [5] or Proximal Policy Optimization (PPO) [12], RIS can intelligently adjust beamforming strategies to enhance signal quality and reduce interference. Furthermore, these models can operate with minimal computational overhead during inference, making them well-suited for real-time deployment on Field Programmable Gate Array (FPGA) to handle dynamic wireless environments.

The integration of RL into RIS also offers significant advantages in terms of scalability [11]. The ability to embed these models into constrained physical components, such as the individual elements of a RIS, allows for efficient deployment across large-scale networks. This scalability is essential for future network infrastructures, where adaptability and efficiency are paramount. As networks become more densely populated with devices and users, the need for intelligent real-time optimization becomes increasingly important. RL provides a powerful framework for achieving this optimization, making

it an attractive solution for next-generation wireless networks.

However, RL integration into RIS also presents new security challenges that must be addressed. Deep learning models, which underpin many RL algorithms, are often criticized for their lack of explainability [14]. The *black-box* nature of deep learning models makes it difficult to understand the decision-making processes of these models, creating potential vulnerabilities that can be exploited by malicious actors. For example, adversaries could manipulate the environment in ways that cause the RL model to make suboptimal decisions, leading to degraded network performance or even security breaches [8]. Therefore, it is crucial to conduct thorough studies to identify and mitigate these vulnerabilities, ensuring the robustness of RL-driven RIS.

III. Research Directions

Our research is focused on the following key areas to address the aforementioned challenges and opportunities:

1) **Simulation Environment Development —** We are developing a comprehensive Python-based simulation environment, inspired by the research of Peng et al. [11], for full-duplex communications between a base station (BS) and users via a RIS. This environment will include the presence of eavesdroppers, allowing us to simulate real-world scenarios and test the robustness of DRL models under various conditions. The development of this environment is a critical first step in our research, as it provides a controlled setting for experimentation and validation. By simulating different network conditions and attack scenarios, we can better understand the strengths and weaknesses of DRL-driven RIS.

2) **Attack Schemes and Vulnerability Analysis —** To evaluate the robustness of our RL model, we will explore various attack schemes that manipulate the environment. Eavesdroppers, assumed to be entirely passive, will employ mobility patterns to disrupt the RIS. They may also use intelligent positioning strategies, using their own RL or Multi-Agent Reinforcement Learning (MARL) algorithms [1] to maximize their impact. By understanding these attack vectors, we can develop more resilient DRL models to operate the RIS. This involves analyzing how different attack strategies affect the performance and security of the RIS and developing countermeasures to mitigate these risks.

3) **Defense Mechanisms and Mitigation Techniques —** To address the vulnerabilities identified in the AI controller of the RIS, we will develop and implement robust defense mechanisms. This includes redesigning the reward mechanism of the DRL agent to better align with the goals of ensuring both safety and optimal performance for each user. Additionally, we will explore architectural enhancements, such as integrating RNNs or LSTMs, to enhance reliability. We will also employ adversarial training with a second AI agent designed to identify and exploit vulnerabilities. Curriculum Learning (CL) [2] [3] for RL is another promising approach to reduce training time by gradually introducing more complex scenarios. Furthermore, we will refine the simulation environment and address specific attack schemes targeting the AI model, such as environment poisoning (altering the environment from the AI system's perspective) and reward poisoning.

4) **Findings —** To ensure the rigor and reliability of our findings, we propose to conduct a thorough statistical analysis of the results obtained from our simulations and experiments. We would employ methods such as those described in [4]. This approach could potentially allow us to make meaningful comparisons between different RL algorithms and evaluate their performance under various conditions. By applying robust statistical techniques, we aim to draw valid conclusions about the effectiveness and resilience of DRL models in RIS, potentially providing a solid foundation for future research and practical implementations.

5) **Transitioning to Real Testbeds —** After successfully achieving reliable results from our simulations, our next objective is to test our system in real-world conditions using prototypical RIS developed for the PEPR Future Network project. This transition to physical testbeds is crucial for validating our theoretical findings and ensuring the practical viability of our solutions. We will proceed with this phase of testing as soon as these systems, which are currently under development, become available. It is important to note that RIS technology is still in its nascent stages.

IV. Conclusion

The purpose of our research is to investigate the potential vulnerabilities of the RL systems used to operate RIS. By exploring these attack vectors and their consequences, we aim to contribute to the development of more secure and robust communication networks. Our work lays the foundation for future research in this area, paving the way for more resilient and adaptive use of DRL to operate RIS. As wireless networks continue to evolve, it will be crucial to ensure the security and efficiency of RIS will be crucial to realize the full potential of these advanced technologies.

Acknowledgments The work is supported by the French National Research Agency under the France 2030 label (NF-HiSec ANR-22-PEFT-0009).

References

[1] Stefano V Albrecht, Filippos Christianos, and Lukas Schäfer. *Multi-agent reinforcement learning: Foundations and modern approaches*. MIT Press, 2024.

[2] Yoshua Bengio, Jérôme Louradour, Ronan Collobert, and Jason Weston. Curriculum learning. In *Proceedings of the 26th annual international conference on machine learning*, pages 41–48, 2009.

[3] Walter Brescia, Luca De Cicco, and Saverio Mascolo. Sample-efficient reinforcement learning for pose regulation of a mobile robot. In *2022 11th International Conference on Control, Automation and Information Sciences (ICCAIS)*, pages 42–47. IEEE, 2022.

[4] Cédric Colas, Olivier Sigaud, and Pierre-Yves Oudeyer. A hitchhiker's guide to statistical comparisons of reinforcement learning algorithms, 2022.

[5] Stephen Dankwa and Wenfeng Zheng. Twin-delayed ddpg: A deep reinforcement learning technique to model a continuous movement of an intelligent robot agent. In *Proceedings of the 3rd international conference on vision, image and signal processing*, pages 1–5, 2019.

[6] ETSI ISG RIS. ETSI GR RIS 001 V1.2.1: Reconfigurable Intelligent Surfaces (RIS); Use Cases, Deployment Scenarios and Requirements. Technical Report V1.2.1, European Telecommunications Standards Institute (ETSI), February 2025.

[7] Chongwen Huang, Ronghong Mo, and Chau Yuen. Reconfigurable intelligent surface assisted multiuser miso systems exploiting deep reinforcement learning. *IEEE Journal on Selected Areas in Communications*, 38(8):1839–1850, 2020.

[8] Inaam Ilahi, Muhammad Usama, Junaid Qadir, Muhammad Umar Janjua, Ala Al-Fuqaha, Dinh Thai Hoang, and Dusit Niyato. Challenges and countermeasures for adversarial attacks on deep reinforcement learning. *IEEE Transactions on Artificial Intelligence*, 3(2):90–109, 2021.

[9] Timothy P Lillicrap, Jonathan J Hunt, Alexander Pritzel, Nicolas Heess, Tom Erez, Yuval Tassa, David Silver, and Daan Wierstra. Continuous control with deep reinforcement learning. *arXiv preprint arXiv:1509.02971*, 2015.

[10] Yuanwei Liu, Xiao Liu, Xidong Mu, Tianwei Hou, Jiaqi Xu, Marco Di Renzo, and Naofal Al-Dhahir. Reconfigurable intelligent surfaces: Principles and opportunities. *IEEE communications surveys & tutorials*, 23(3):1546–1577, 2021.

[11] Zhangjie Peng, Zhibo Zhang, Lei Kong, Cunhua Pan, Li Li, and Jiangzhou Wang. Deep reinforcement learning for RIS-aided multiuser full-duplex secure communications with hardware impairments. *IEEE Internet of Things Journal*, 9(21):21121–21135, 2022.

[12] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, and Oleg Klimov. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*, 2017.

[13] Richard S. Sutton and Andrew G. Barto. *Introduction to reinforcement learning*. MIT Press, 2 edition, 2012. (draft 2nd ed.).

[14] George A Vouros. Explainable deep reinforcement learning: state of the art and challenges. *ACM Computing Surveys*, 55(5):1–39, 2022.