Integrating Reconfigurable Intelligent Surfaces into Next-Generation Mobile Networks: Comparative Simulations Based on Simu5G

Wenqing Dai[1], Christoph Lipps[1] and Hans Schotten[1,2]
[1]Intelligent Networks Research Group, German Research Center for Artificial Intelligence, Kaiserslautern, Germany
[2]Institute for Wireless Communication and Navigation, RPTU University Kaiserslautern-Landau, Germany

Wenqing.Dai@dfki.de
Christoph.Lipps@dfki.de
Hans_Dieter.Schotten@dfki.de

Abstract: Due to the need for high-performance communication systems capable of supporting a wide range of applications -including industrial automation, smart healthcare, and autonomous driving-, Next-Generation Mobile Networks (NGMNs) are continuing to evolve. Furthermore, to cope with variable traffic situations in urban vehicular environments, autonomous cars require communication, high reliability, doubtless integrity and low latency. Besides, in smart city environments, an AI-powered attack can i) exploit vulnerabilities in connected autonomous vehicles by generating spoofed signals to misdirect navigation and orchestrating jamming attacks to disrupt Vehicle-to-Everything (V2X) communications; In the same way, ii) telemedicine applications and wearable medical devices in the healthcare industry require reliable and secure communication in dynamic, interference-prone indoor and outdoor environments. However, in order to facilitate synchronized Machine-to-Machine (M2M) operations under strict latency and reliability limitations, industrial automation relies on resilient and robust wireless communication. In this context, Reconfigurable Intelligent Surfaces (RISs) have emerged as one of the potential Sixth Generation (6G)-enabling technologies capable of addressing these challenges. By dynamically reconfiguring the wireless propagation environment through programmable surfaces, RISs can improve the system performance in terms of signal reliability, coverage, and energy efficiency. To examine this, this work focuses on comparative simulations evaluating the network-layer performance of RIS-enhanced and non-RIS networks using the network simulation environment *Simu5G*. Thereby, key RIS features, such as channel optimization and interference suppression, are modelled to assess their impact on critical metrics like Signal-to-Interference-plus-Noise-Ratio (SINR), resilience, and secrecy efficiency against adversarial threats. Furthermore, this work highlights how RISs can mitigate security risks such as eavesdropping, spoofing, and jamming, which are becoming increasingly prevalent in AI-driven attack scenarios. For instance, RISs effectively counters AI-generated spoofed signals in autonomous vehicle networks and suppresses jamming in V2X communication. Comparative results demonstrate the superiority of RIS-enabled network architectures in both performance and security. In addition, the work provides academic and industrial researchers with a robust toolkit for examining the dual function of RIS in improving wireless network performance and security by expanding the Simu5G platform with RIS-capable modules. This contribution is an important step towards enabling real-world deployment of RIS in future networks.

Keywords: Reconfigurable intelligent surfaces, Next generation mobile networks, Cyber security, Beyond 5G, 6G, Network simulations

1. Introduction

The transition to the Fifth Generation (5G) of mobile networks has significantly advanced the capabilities of wireless communication, offering enhanced data rates, reduced latency, and massive connectivity for a multitude of different applications. However, these gains are accompanied by complex challenges in ensuring reliable and secure communication, particularly in urban environments characterized by high user density, diverse propagation scenarios, and increased vulnerability to cyber threats. Conventional network architectures face limitations in delivering secure and high-quality connectivity across such heterogeneous environments, where physical obstacles and interference often impair signal quality and coverage (CISCO, 2017). Considering this, various so-called enabling technologies are being proposed for the upcoming networks and wireless standard of Beyond 5G (B5G) and the Sixth Generation (6G).

In particular Reconfigurable Intelligent Surfaces (RISs) have emerged as one of these promising technologies to address certain challenges. Basically, they are “planar metasurfaces with a large array of passive, reconfigurable elements” (Pan et al, 2021), capable of dynamically control the properties of incident electromagnetic waves, including phase, amplitude, and direction. Further approaches to adjusting the reflection characteristics are to physically or mechanically change the orientation and position of some of the elements and research activities related to metamaterials and liquid crystals, which are technologically more sophisticated. By adapting the material properties such as permittivity, permeability, and conductivity, the reflection behaviour and radiation characteristics of the RIS can be adjusted as well. By tailoring the reflection and transmission characteristics of these surfaces, this technique can effectively manipulate wireless propagation environments to enhance communication performance and Physical Layer Security (PLS). As indicated in Figure 1, RISs enables various wireless transmission methods in the current networks. This extends from ground applications and the expansion of coverage to communication links at sea, in the air, and even in space. Moreover, there are potential integrations with applications such as Visible Light Communication (VLC) (Rüb et al, 2024) and millimeter Wave (mmWave) (Qiao & Alouini, 2020) technology. All these areas and interfaces have a considerable need for security and the confidential transmission of data. This is exactly where RIS can contribute as well.

The RIS technology aligns with the evolving demands of Beyond 5G applications in sectors such as autonomous vehicles, industrial automation, and smart cities. Especially in Non-Line-of-Sight (NLoS) scenarios, the integration of RISs into the existing network infrastructure will create an alternative path from the transmitter and receiver. Therefore, the development and implementation of RISs within simulation environments like *Simu5G* is thus an essential step towards understanding and realizing the potential of the technology and in securing B5G networking.

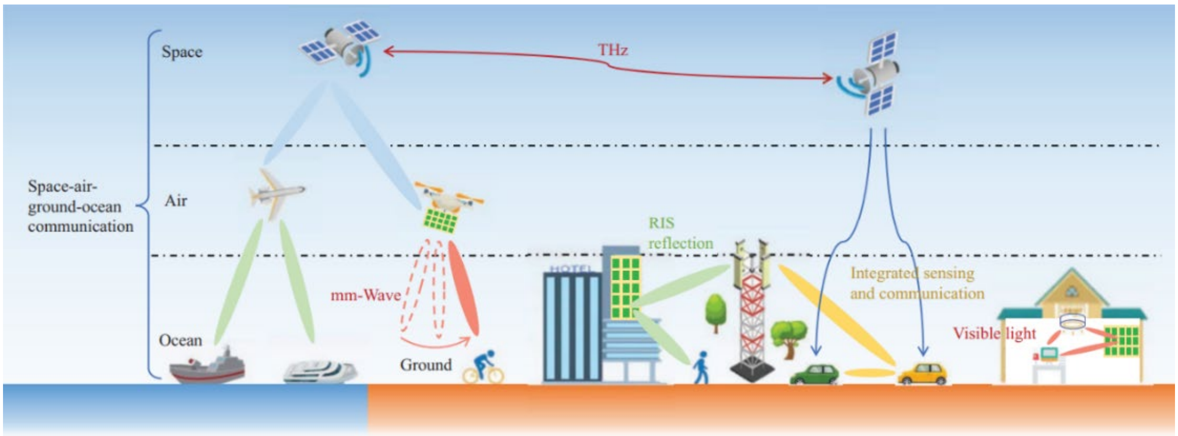

Figure 1: The broad potential for RIS implementations in 6G with use cases in indoor (VLC), urban, but also non-terrestrial and open sea applications (Xu et al, 2023)

To enable the requirements of the above-mentioned use cases, there are in particular the following aspects motivating the integration of RIS into B5G and 6G networks.:

- Enhanced Physical Layer Security: This technology can -among others-, direct signals toward legitimate receivers and away from unintended ones, thereby reducing the risk of interception and enhancing the security of the communication channel (Lipps et al, 2022). This ability to control the propagation path at the physical layer represents a promising approach to mitigating eavesdropping risks, particularly in scenarios where traditional encryption methods are insufficient or cost-prohibitive.
- Improved Signal Quality and Coverage: By dynamically shaping the propagation environment, RIS can mitigate the effects of obstacles, multipath fading, and non-line-of-sight conditions, which are prevalent in dense urban environments. This capability enables more robust and consistent signal coverage, facilitating secure communication even in challenging scenarios with complex physical obstructions.
- Energy Efficiency: Unlike traditional active relays or amplifiers, RIS elements are passive and require minimal power for operation. This property makes RIS a sustainable and cost-effective solution for extending network reach and enhancing signal quality without incurring significant energy costs, aligning with the energy efficiency goals of modern network design.
- Adaptability to Dynamic Environments: RIS can be reconfigured in real-time to adapt to variations in user location, interference patterns, and environmental conditions. This flexibility allows for the optimization of signal paths on demand, ensuring high quality of service and secure connectivity for mobile users in dynamic and unpredictable settings.

The of the work is organized as follows: Section 2 provides a brief introduction to the current state of RIS research and technology in relation to security applications and network simulation platforms. In addition, Section 3 introduces the implementation process of RIS integrated into the existing network on this platform. The result from the simulation is analysed and discussed in Section 4. Section 5 summarizes the work and gives an overview of future work.

2. Related Work

The transition to a hyperconnected, all-electric world of tomorrow emphasizes how essential secure data transmission will become in the future. It is not only an increasing amount of data being sent via the communication infrastructure, but the value of the data is increasing as well. In addition to data critical to companies (sensor data, capacity utilization, etc.) and Intellectual Property (IP), personal and health data will be transmitted. To address this, there are already a number of countermeasures and approaches to improve security, such as methods for homomorphic encryption (Sanon, Lipps and Schotten, 2023) -to operate and learn on encrypted data- as well as developments in zero trust (Nahar et al., 2024), network slicing (Singh et al. 2024), quantum cryptography and Post-Quantum Security (PQS) (Mansoor et al., 2024).

Furthermore, there are approaches for security on the physical layer, so-called Physical Layer Security, which, among others, use the physical characteristics of the transmission channel to increase security. This is an area in which the Reconfigurable Intelligent Surfaces -which are the main focus of this work-, can also make a contribution: RISs can improve security without requiring significant changes of the systems. They can, for instance, use PLS approaches to lessen channel correlation between authorized users and eavesdroppers by rearranging the electromagnetic environment. In addition to providing affordable, energy-efficient, and readily deployed solutions for secure networks in a variety of settings, this integration enhances communication security (Naeem et al, 2023) (Chen et al, 2021) (Yang et al, 2020).

Therefore, for example, the work of *Huang et al.* (2021) address the Pilot Contamination Attack (PCA). By proposing a Generalized CUmulative SUM (GCUSUM) detection method with zero-forcing beamforming, they are able to reduce the signal leakage and enhance the secure transmission. Furthermore, for pilot spoofing attacks, it is suggested to use RISs near to legitimate users to disrupt the channel reciprocity by controlling phase shifts, and biasing beamforming against eavesdroppers (Yang et al, 2021). A Three-Step Training (TST) scheme is introduced by *Liu et al.* to detect Pilot Spoofing Attack (PSA) by analyzing signal power levels, enabling CSI estimation for legitimate and spoofed channels without prior noise variance knowledge (2021).

To counter jamming attacks, *Tang et al.* (2021) propose to use Aerial-RIS for flexible deployment and optimized beamforming, while *Tu et al*. (2024) introduced dynamic RISs deployment to enhance secrecy and reduce complexity. Moreover, RISs are explored as green jammers, using reflected signals to disrupt communication through destructive interference (Lyu et al,2020). Furthermore, a Non-Orthogonal Multiple Access (NOMA)-assisted cognitive radio IoT network using STAR-RIS to enhance indoor communication is also proposed under power constraints and eavesdropping threats (Li et al, 2023), whereas *Zhang et al.* addressed full-space eavesdropping with a secure beamforming design for STAR-RIS, achieving higher secrecy capacity than conventional RISs (2023).

Guan, Wu, and Zhang (2020) as well as *Hong et al*. (2020) explore how Artificial Noise (AN) benefits the secure wireless network. By dividing RIS elements into two virtual partitions: one to enhance legitimate signals and the other to amplify AN's impact on attackers, the secrecy capacity is significantly improved (Arzykulov et al, 2023). Besides, to counter RISs misuse by attackers (IRIS), *Wang et al.* (2022) introduce an AN-aided joint optimization solution, effectively mitigating IRIS's impact on PLS.

A novel threat to physical-layer signals, the Environment Reconfiguration Attack (ERA), is introduced by *Staat et al. (2022)*. By manipulating existing signals through RIS, legitimate receivers were disrupted without the emission of new signals or the need for channel knowledge. Besides, *Hu et al.* (2021) described a similar RIS-assisted Manipulating attack (RISM), which interfered with Physical-layer Key Generation (PKG) by altering channel reciprocity through rapid RIS reflection coefficient changes during OFDM channel probing.

In the domain of V2X communication, much of the research has focused on extending area coverage in urban environments, such as around building corners or in blind regions. However, the increasing amount of data exchanged between vehicles and their surroundings has also become a target for attackers. To counter eavesdropping threats, *Ayza et al.* (2023) proposed methods to improve communication confidentiality, which include deriving closed-form expressions for Secrecy Outage Probability (SOP).

Various simulation tools have been employed to explore RIS capabilities in complex network scenarios. Among these, OMNeT++, an open-source discrete-event network simulation framework, has been widely utilized.

Known for its modularity, it allows communication networks to be modelled and tested under controlled conditions, making it particularly suitable for V2X scenarios. The RIS research has also been advanced through CoopeRIS, a framework developed by *Segata et al.* (2024). This framework, integrated with Plexe/Veins/SUMO, supports the study of RIS-assisted mmWave communications and addresses challenges such as non-line-of-sight (NLoS) links in vehicular environments. Multi-user service delivery has been facilitated, and RIS's potential in connected vehicle communications has been demonstrated through this tool's component-based architecture.

Simu5G, an extension of OMNeT++, is specifically designed to simulate 5G networks. Built on the INET framework, it provides enhanced capabilities for modeling 5G New Radio (NR) features, such as flexible frame structure, dynamic resource allocation, and Ultra-Reliable Low-Latency Communication (URLLC). *Simu5G* supports the detailed modeling of 5G-specific elements, including Next-generation Base stations (gNBs), User Equipment (UE), and various 5G applications. This makes Simu5G particularly well-suited for investigating RIS's impact on 5G networks, as it provides the necessary infrastructure to simulate high-density environments, interference management, and the demands of low-latency applications.

3. RIS Module Design and Integration

The integration of RIS into the network simulation platform necessitates a carefully structured module architecture, informed design choices, and a strategic approach to ensure accurate modelling and seamless operation within the existing 5G simulation framework. The RIS module is designed to represent the essential functionalities and behaviors of RIS technology, enabling the simulation of its impact on wireless propagation, signal quality, and security in 5G networks.

3.1 Key Design Choices

To ensure the functionality and compatibility of the RIS modules with the existing simulation platform, various design decisions are made:

- Realistic Propagation Modelling: One of the fundamental design choices is to implement a detailed propagation model capturing the phase shifting, beamforming, and wavefront manipulation capabilities of RIS. The model considers key factors such as angle of incidence, distance from the RIS, and environmental parameters. This approach enables realistic simulation of RIS-enhanced paths, accounting for the directional focus and interference suppression that RIS technology can provide.
- Dynamic Reconfiguration Capability: To reflect the adaptive nature of RIS, the module is designed with real-time reconfiguration capabilities. Thereby, the RIS Controller can dynamically adjust the configuration of the RIS Surface Array in response to changing network conditions, such as user movement or fluctuations in interference. This reconfigurability is essential for simulating the role of RIS in environments requiring dynamic adaptation, such as vehicular networks or urban areas with high user mobility.
- Interfacing with Simu5G Protocols: The integration is structured to align with existing Simu5G protocols and network entities, ensuring that the RIS module operates coherently within the Simu5G framework. This compatibility allows the RIS module to interact with gNBs, UEs, and other network elements, enabling comprehensive performance evaluations. The module's design also supports communication with *Simu5G's* resource allocation and scheduling algorithms, allowing for joint optimization of network resources and RIS configuration.
- Performance Efficiency: Given the computational demands of simulating numerous RIS elements, the module is optimized to reduce simulation complexity without sacrificing accuracy. This is achieved by grouping RIS elements into clusters for certain propagation calculations, a design choice that balances accuracy and computational efficiency, enabling large-scale simulations within reasonable timeframes.

3.2 Simulation Environment

The simulation environment is described in this section. The simulation focuses primarily on the single-cell, single-user scenario, as illustrated in Figure 2. Utilizing the signal enhancement feature of RISs for mobile communication and the suppression feature of unauthorized user signals, the influence of the user's distance from the base station on system performance is examined in this scenario.

3.2.1 Module architecture

The primary focus of the initial design is the passive reflection functionality of RISs. As their fundamental purpose is to reshape the electromagnetic field and thereby enhance the signal strength and coverage of wireless communication, consequently, this module construction begins with the channel module to address this core capability.

Figure 2: V2X use case where RIS can aid against jamming attacks

To analyze the transmission of information between different layers of the mobile network, the existing *channelControl* module in the simulation platform is used as a starting point. Since passive RISs operates solely within the physical layer, extending the functionality of the *channelControl* module is a natural and logical choice.

The RIS module is constructed with key attributes and functionalities. These include defining its position within the network, specifying the number of reflective elements, quantifying the amplitude of reflected signals through reflection coefficients, and introducing adjustable phase shifts for signal reflection. These parameters collectively determine RIS's behavior and influence on the communication environment.

The control file of the RIS module defines its operations within the network and facilitates the analysis of information transfer between layers. This includes specifying basic variables such as the operating frequency band, system loss parameters, and wavelength. Functions are incorporated to retrieve the locations of radio signal transmitters and receivers, calculate wireless transmission loss, model signal loss through the RIS, and compute the security rate of the communication link (see Table 2).

This structured approach ensures seamless progression from the analysis of existing modules to the development of a fully functional RIS module, providing a robust foundation for further enhancements and optimizations.

Table 2: Initial parameters in simulation network from Figure 2

Network paramters	
Map size	1000 × 1000
Number of subchannels	50
UE transmission power	26
eNodeB transmission power	40
eNodeB location	(500, 500)
Number of UE	1
UE location	(350, 450)

Network paramters	
Wireless channel attenuation	2.0
System loss	1.0
RIS location	(400, 500)
RIS reflectionCoefficient	1.5
RIS phase shift	0.3 in radians

3.2.2 *Simulation workflow*

The procedure for RIS-aided transmission workflow is as follows: It begins by initializing several parameters. These include the reflection coefficient, representing the efficiency of the RIS in reflecting signals, and the phase shift, which accounts for the adjustment applied to the signal by the RIS. The position of the RIS is specified, along with the signal's carrier frequency, propagation speed (e.g., the speed of light), a system loss factor accounting for inefficiencies, and the wavelength, which is derived from the propagation speed and frequency.

Once the parameters are set, the main workflow proceeds by calculating the distances between the system's key components. These distances encompass the distance between the transmitter and the RIS, the RIS and the receiver, and, if relevant, the RIS and a potential eavesdropper. Using these distances, the path loss for each communication link is calculated using free-space path loss formulae. This accounts for the attenuation of signals as they travel down each path. Next, the signal power is measured at both the receiver and the eavesdropper. At the receiver, power is determined by adding the path of losses from the transmitter to the RIS and from the RIS to the receiver. Similarly, the eavesdropper's signal power is calculated by adding the route losses from the transmitter to the RIS and then from the RIS to the eavesdropper.

If the eavesdropper's position is known, the secrecy capacity is computed to assess the security of the communication channel. This is accomplished by comparing the capacity of the legitimate receiver to that of the eavesdropper, with the legitimate receiver having a higher capacity. The following formula gives the secrecy capacity:

$$C_s = \max\left(0, \log_2\left(1 + \frac{P_{R_X}}{\sigma^2}\right) - \log_2\left(1 + \frac{P_{Eavesdropper}}{\sigma^2}\right)\right),$$

where P_{Rx} and $P_{Eavesdropper}$ are the signal powers at the receiver and eavesdropper, respectively, and σ^2 is the noise variance.

The results of this analysis, including SINR, received signal power, and the secrecy capacity, are output. The process is then repeated for the next transmission cycle, with updated parameters or positions as necessary. This iterative approach ensures comprehensive evaluation of the RIS-aided transmission system.

4. Result Analysis and Discussion

Since the RIS-supported channel model mentioned in this work is based on the existing *channelControl* in the platform and has added RIS parameters in the functional files, this section will compare the standard *channelControl* in the platform with the RIS channel integrated based on it.

The simulation is set up with 50 subchannels to simulate multipath transmission in wireless networks. Firstly, the basic performance received power, and SINR are analyzed. It can be seen in Figure 3 and Figure 4 that in the mobile network with RIS assistance, the received signal and SINR are significantly improved compared to the unassisted communication, although the disparity still exists in the different subchannels.

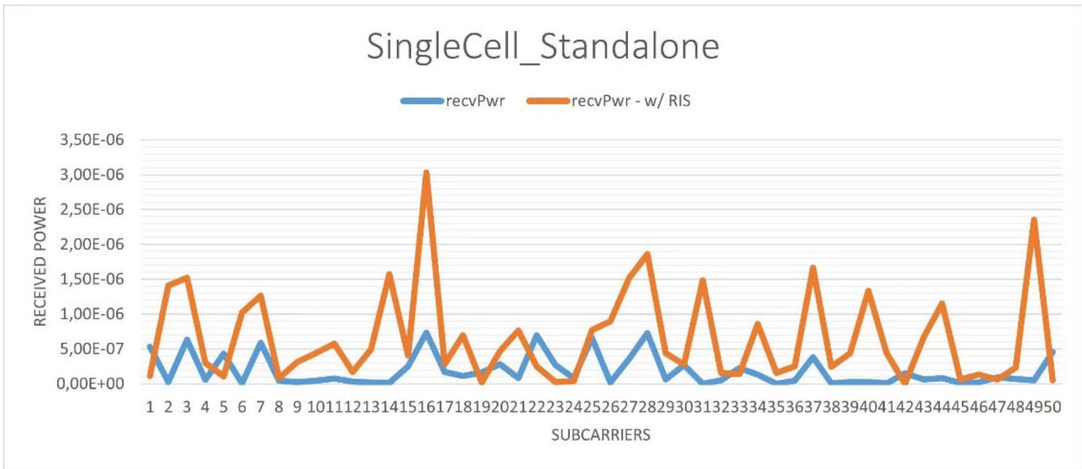

Figure 3: V2X use case where RIS can aid against jamming attacks

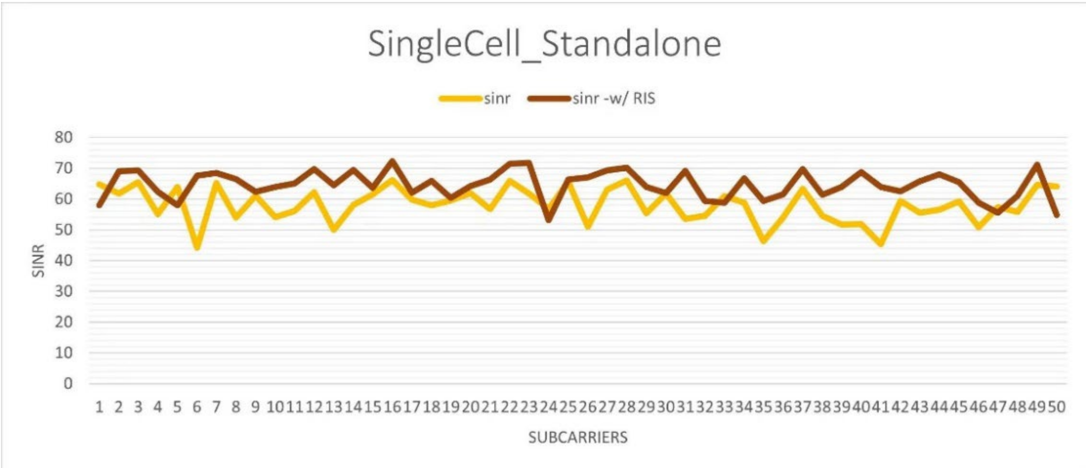

Figure 4: Comparative SINR between RIS-aided channel and *channelControl*

The secrecy rate (in bits per channel use) is analysed for two scenarios: with and without RIS, considering an eavesdropper in a single-cell setup. With RIS, the secrecy rate remains consistently high (0.9 bits per channel use), indicating enhanced secure communication. Without RIS, it is significantly lower (0.3-0.4 bits), highlighting increased vulnerability to eavesdropping. RIS effectively improves secrecy across all subchannels, as shown by the persistent gap between the two curves in Figure 5.

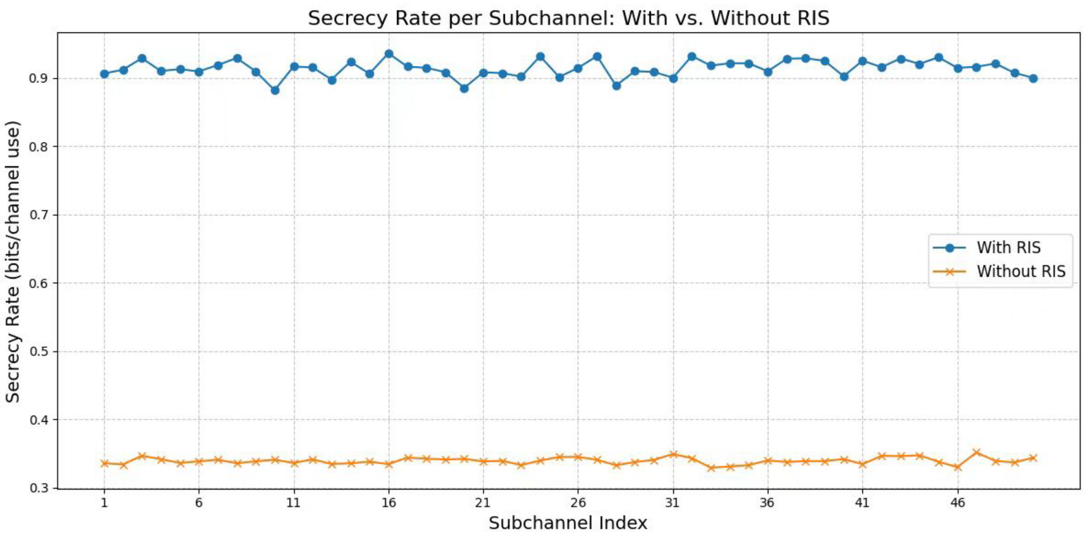

Figure 5: Comparative secrecy rate between RIS-aided channel and *channelControl*

The secrecy rate (in bits per channel use) was analysed for two scenarios: with and without RIS, considering an eavesdropper in a single-cell setup. With RIS, the secrecy rate remains consistently high (0.9 bits per channel use), indicating enhanced secure communication. Without RIS, it is significantly lower (0.3-0.4 bits), highlighting increased vulnerability to eavesdropping. RIS effectively improves secrecy across all subchannels, as shown by the persistent gap between the two curves in Figure 5.

To summarize, the results show that incorporating the RIS module in the simulation platform can be an effective strategy to integrate it into the wireless communication network. In upstream and downstream communication, RIS can significantly improve signal strength and SINR at the receiving end. By including the secrecy rate estimated with the eavesdropper attack in its control file, the results show that RIS can significantly increase system security as well. The afterwards processing of the security rate reveals that RIS introduces more transmission pathways in the system, resulting in a significant increase in system variability when compared to the system without RIS assistance, i.e., system consistency is insufficient. This can be improved by involving more channel estimation techniques and so on.

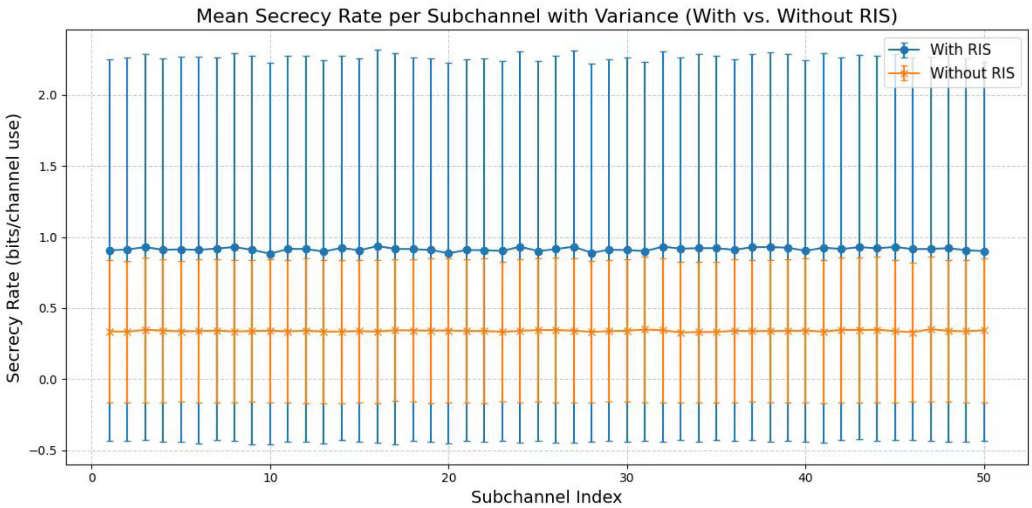

Figure 6: Comparative mean secrecy rate with variance between RIS-aided channel and *channelControl*

Furthermore, due to the main objective of this network simulation platform is to simulate information transmission in the network, the definition of the characteristics and principles of physical layer signal transmission is not straightforward or simple enough, and further research and development in this field will be valuable.

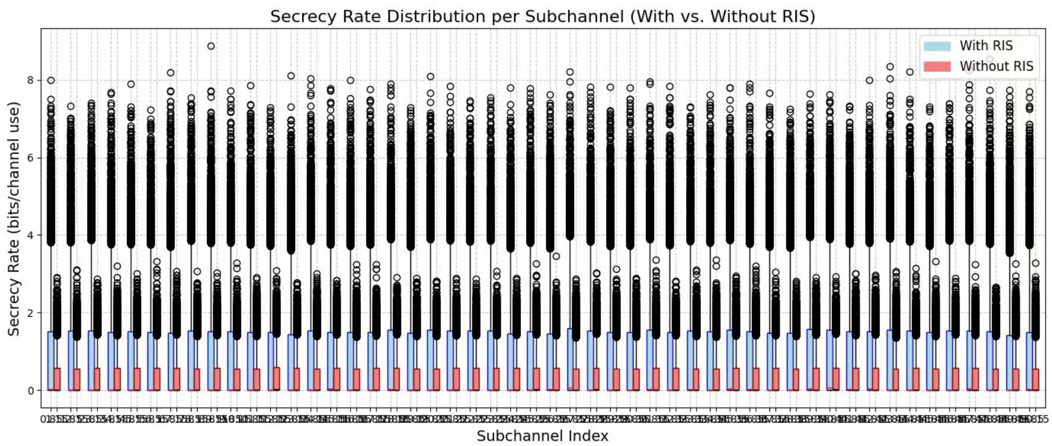

Figure 7: Comparative secrecy rate distribution between RIS-aided channel and *channelControl*

5. Conclusion and Future Work

In a hyper-connected future, there will not just be more and more end devices and communication participants integrated into the networks, but also an increasing volume of ever more sensitive data being transmitted. This poses particular challenges for the integrity of this data, but also for the security and resilience of the communication infrastructure. In addition to traditional security mechanisms such as encryption and authentication, approaches such as zero trust, homomorphic encryption and security arising in the context of so-called 6G-enabling technologies such as Reconfigurable Intelligent Surfaces are shifting into the focus of academia and research as part of the development of sixth-generation mobile communications.

In this context, this work investigates approaches to integrate and simulate RISs with the network simulation platform *Simu5G*, expanding the potential of network simulations in the context of wireless communication systems of the future. The application demonstrates how the RIS technology can boost performance parameters including signal strength, energy efficiency, and network stability by dynamically reconfiguring the wireless environment. The results of the simulations prove that the integration of RIS modules can be an effective method of integrating them into wireless networks. RISs can significantly enhances signal strength by a factor of up to 5–6 times at its peaks, SINR by approximately 10–20 dB on average, and nearly double the system security rate, particularly by mitigating eavesdropper attacks through increased secrecy rates. However, the analysis reveals that RISs introduces additional transmission pathways, leading to increased system variability and reduced consistency compared to systems without RIS.

By bridging the gap between RIS theoretical models and practical network simulations, this work provides a foundational tool for researchers and developers to further analyze RIS's potential in real-world 5G and beyond applications. The modular approach adopted ensures flexibility, allowing for seamless integration to evolving standards and technologies.

Future research can build on this foundation by investigating RIS's involvement in connected mobility and autonomous driving by multi-RIS deployments, AI-based RIS optimization algorithms, and interaction with vehicular networks. The incorporation of RIS into simulation systems such as OMNeT++ and Simu5G will be essential in promoting innovation and speeding up research as wireless communication develops further. In addition, the simulations are compared with results from the real world in order to evaluate the simulation results in this direction as well.

With these contributions, this study not only highlights RIS's transformative potential but also offers a platform for more research in this area.

Acknowledgement

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16KIS2239K SUSTAINET_guarDian and 16KIS1398K Open6GHub). The authors alone are responsible for the content of the paper.

References

Arzykulov, S., Celik, A., Nauryzbayev, G. and Eltawil, A. M., "Artificial Noise and RIS-Aided Physical Layer Security: Optimal RIS Partitioning and Power Control," *IEEE Wireless Communications Letters*, vol. 12, no. 6, pp. 992-996, DOI: 10.1109/LWC.2023.3256001, 2023.

Ayaz, H., Waqas, M., Abbas, G., Abbas, Z. H., Bilal, M., “Multiple re-configurable intelligent surfaces based physical layer eavesdropper detection for V2I communications.” *Physical Commun*ication, vol. 58, ISSN 1874--4907, DOI: 10.1016/j.phycom.2023.102074, 2023.

Chen, Q., Li, M., Yang, X., Alturki, R., Alshehri, M. D. and Khan, F., “Impact of Residual Hardware Impairment on the IoT Secrecy Performance of RIS-Assisted NOMA Networks,” *IEEE Access*, vol. 9, pp. 42 583--42 592, DOI: 10.1109/ACCESS.2021.3065760, 2021.

CISCO (2017) Cisco Annual Internet Report (2018-2023), Cisco public White paper.

Guan, X., Wu, Q., and Zhang, R., "Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?", *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 778--782, DOI: 10.1109/LWC.2020.2969629, 2020.

Hong, S., Pan, C., Ren, H., Wang, K. and Nallanathan, A., "Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface", *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851--7866, Dec. 2020, DOI: 10.1109/TCOMM.2020.3024621, 2020.

Hu, L., Li G., Hu, A. and Kwan, Ng. D. W., “Exploiting Malicious RIS for Secret Key Acquisition in Physical-Layer Key Generation”, *IEEE Wireless Communications Letters,* vol. 13, pp. 417--421, DOI: 10.1109/LWC.2023.3330809, 2024.

Huang, K.-W. and Wang, H.-M., “Intelligent Reflecting Surface Aided Pilot Contamination Attack and Its Countermeasure”, *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 345--359, DOI: 10.1109/TWC.2020.3024808, 2021.

Li, X., Zhang, J., Han, C., Hao, W., Zeng, M., Zhu, Z., and Wang, H., “Reliability and Security of CR-STAR-RIS-NOMA Assisted IoT Networks”, *IEEE Internet of Things Journal,* DOI: 10.1109/JIOT.2023.3340371, 2023.

Lipps, C. and Schotten, H. D., “Physical Layer Security: About Humans, Machines and the Transmission Channel”, *21st European Conference on Cyber Warfare and Security (ECCWS)*, Chester, United Kingdom (UK), DOI: 10.34190/eccws.21.1.403, 2022.

Lipps, C., Herbst, J., Reddy, R., Franke, L., Becker, S., Rahm, M., Schotten, H. D., “Reconfigurable Intelligent Surfaces: A Physical Layer Security Perspective”, *4th International Conference on Data Intelligence and Security (ICDIS)*, Shenzhen, China, 2022, pp. 174--181, DOI: 10.1109/ICDIS55630.2022.00034, 2022.

Lipps, C., Dai, W., Munoz, Y. and Schotten, H.D., “Reconfigurable Intelligent Surfaces and How They Contribute to Security and Privacy”, *IEEE International Conference on Communications and Network Security (IEEE CNS),* Taipei, Taiwan, 2024.

Lipps, C., Herbst, J., Klingel, S., Franke, L., Wolff, A., Rüb, M., Reddy, R., Rahm, M. and Schotten, H. D., “Connectivity in the Era of the (I)IoT: About Security, Features and Limiting Factors of Reconfigurable Intelligent Surfaces”, *Discover the Internet of Things*, vol. 3, no. 16, DOI: 10.1007/s43926-023-00046-1, 2023.

Liu, X., Tao, Y., Zhao, C. and Sun, Z., "Detect Pilot Spoofing Attack for Intelligent Reflecting Surface Assisted Systems", *IEEE Access*, vol. 9, pp. 19228--19237, DOI: 10.1109/ACCESS.2021.3054821, 2021.

Lyu, B., Hoang, D. T., Gong, S., Niyato, D. and Kim, D. I., "IRS-Based Wireless Jamming Attacks: When Jammers Can Attack Without Power", *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1663--1667, DOI: 10.1109/LWC.2020.3000892, 2020.

Manssor, K., Afzal, M., Iqbal, W. and Abbas, Y., “Securing the Future: Exploring Post-Quantum Cryptography for Authentication and User Privacy in IoT Devices”, *Clustering Computing*, vol. 28, no. 93, DOI: 10.1007/s10586-024-04799-4, 2025.

Munoz, Y., Dai, W., Rüb, M., Herbst, J., Reddy, R., Lipps, C. and Schotten, H. D., “Modular Reconfigurable Intelligent Surfaces: Towards an Application-Adaptive Implementation,” *27th ITG-Symposium Mobile Communication - Technologies and Applications*, Osnabrueck, Germany, pp. 17—23, 2023.

Nahar, N., Andersson, K., Schelén, O. and Saguna, S., „A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks“, *IEEE Access*, vol. 12, pp. 94753—74764, DOI: 10.1109/ACCESS.2024.3425350, 2024.

Naeem F., Ali, M., Kaddoum, G., Huang, C. and Yuen, C., "Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges", *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1196--1217, 2023, DOI: 10.1109/OJCOMS.2023.3273507, 2023.

Pan, C., Ren, H., Wang, K., Kolb, J., Elkashlan, M., Chen, M., Renzo, M. D., Hao, Y., Wang, J., Swindlehurst, A., You, X., Hanzo, L., “Reconfigurable Intelligent Surfaces for 6G Systems: Principles, Applications, and Research Directions,” *IEEE Communications Magazine*, vol. 59, no. 6, pp. 14--20, DOI: 10.1109/MCOM.001.2001076, 2021.

Qiao, J. and Alouini, M. -S., "Secure Transmission for Intelligent Reflecting Surface-assisted mmWave and Terahertz Systems", *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1743--1747, DOI: 10.1109/LWC.2020.3003400, 2020.

Rüb, M., Grüber, J., Lipps, C. and Schotten H. D., "Update Rate and Dimension Requirements for Reconfigurable Mirror Arrays in Vehicular Visible Light Communication," *IEEE 99th Vehicular Technology Conference (VTC2024-Spring),* Singapore, pp. 1--6, DOI: 10.1109/VTC2024-Spring62846.2024.10683665, 2024.

Sanon, S.P., Lipps, C. and Schotten, H.D., “Fully Homorphic Encryption: Precision Loss in Wireless Mobile Communication”, *Joint European Conference on Networks and Communications & 6G Summit*, Gothenburg, Sweden, DOI: 10.1109/EuCNC/6GSummit58263.2023.10188286, 2023

Segata,M., Casari, P., Lestas, M., Papadopoulos, A., Tyrovolas, D. Saeed, T., Karagiannidis, G., Liaskos, C., “CoopeRIS: A Framework for the Simulation of Reconfigurable Intelligent Surfaces in Cooperative Driving Environments,” *Computer Networks,* vol. 248, ISSN 1389-1286, DOI: 10.1016/j.comnet.2024.110443, 2024.

Staat, P., Elders-Boll, H., Heinrichs, M., Zenger, C. and Paar, C., “Mirror, Mirror on the Wall: Wireless Environment Reconfiguration Attacks Based on Fast Software-Controlled Surfaces”, *ACM on Asia Conference on Computer and Communications Security*, ASIA CCS ’22, Nagasaki, Japan: Association for Computing Machinery, pp. 208-221, DOI: 10.1145/3488932.3497767, 2022.

Singh, V.P., Singh, M.P., Hedge, S. and Gupta, M., “Security in 5G Network Slices: Concerns and Opportunities”, *IEEE Access*, vol. 12., pp. 52727—52743, DOI: 10.1109/ACCESS.2024.3386632, 2024.

Tang, X., Wang, D., Zhang, R., Chu Z., and Han Z., "Jamming Mitigation via Aerial Reconfigurable Intelligent Surface: Passive Beamforming and Deployment Optimization", *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6232-6237, June 2021, DOI: 10.1109/TVT.2021.3077662, 2021.

Tu, Q., Dong, Z., Zou, X., Wei, N., Li, Y., Xu, F., “Dynamic reconfigurable intelligent surface deployment for physical layer security enhancement in mmWave systems”, *IET Communications*, vol. 18, no. 5, pp. 365--374. DOI: 10.1049/cmu2.12751, 2024.

Xu, J., Yuen, C., Huang, C., Ul Hassan, N., C. Alexandropoulos, G.C., Renzo, M. D., Debbah, M., “Reconfiguring Wireless Environment via Intelligent Surfaces for 6G: Reflection, Modulation, and Security”, *Science China Information Sciences*, vol. 66, Issue 3, DOI: 10.1007/s11432-022-3626-5, 2023.

Yang, J., Ji, X., Wang, F., Huang K. and Guo, L., “A Novel Pilot Spoofing Scheme via Intelligent Reflecting Surface Based on Statistical CSI”, *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12 847--12 857, DOI: 10.1109/TVT.2021.3120602, 2021.

Yang, L., Yang, J., Xie, W., Hasna, M. O., Tsiftsis, T. and Renzo, M. D., "Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems", in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12296--12300, DOI: 10.1109/TVT.2020.3007521, 2020.

Zhang, Z., Wang, Z., Liu, Y., He, B., Lv, L. and Chen, J., “Security Enhancement for Coupled Phase-Shift STAR-RIS Networks”, *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 8210--8215, DOI: 10.1109/TVT.2023.3243545, 2023.