Optimizing QoS in Secure RIS-Assisted mmWave Network With Channel Aging

Syed Waqas Haider Shah (*Member, IEEE*), Marwa Qaraqe (*Senior Member, IEEE*), Saud Althunibat (*Senior Member, IEEE*), and Joerg Widmer (*Fellow, IEEE*)

***Abstract*—Reconfigurable Intelligent Surfaces (RISs) have demonstrated significant potential in securing mmWave communication from potential eavesdropping by configuring reflecting elements to enhance signal strength at desired locations and create nulls at potential eavesdropping locations. Acquiring perfect channel information is crucial for optimizing RIS configuration; however, obtaining such information is costly and, as a result, should be performed sparingly. This work explores the impact of the age of channel information on secrecy performance when a RIS-assisted mmWave network operates under statistical quality-of-service (QoS) constraints. Specifically, we optimize the QoS performance of a RIS-assisted mmWave network given only outdated channel estimates. To this end, we propose a technique for the joint optimization of transmit beamforming and RIS configuration, along with a closed-form solution for the optimal transmit power control policy. We investigate the impact of channel aging on the performance of these techniques. In our Monte-Carlo simulations, we first identify the factors influencing the aging process of a RIS-assisted mmWave channel in both the near and far fields of the RIS. Subsequently, we examine the impact of channel aging on secrecy capacity and demonstrate that adequate secrecy capacity can still be achieved even when channel information is outdated, reducing the need for frequent RIS configuration. Moreover, our optimal power control policy results reveal that operating in a high SNR regime does not necessarily increase the achievable effective secrecy capacity when the system operates under stricter QoS constraints. This finding allows system designers to adopt a more pragmatic system design approach that consumes less energy while maintaining the required QoS and secrecy performance.**

***Index Terms*—Quality of Service, RIS, mmWave networks, secrecy capacity, effective capacity, outdated channel estimates, age of channel information**

I. Introduction

The 5G mobile communication era is experiencing the dominance of various new applications with enhanced broadband connectivity requirements, which is expected to increase exponentially in the near future. The ever-increasing demand for ultra-high data rate and low-latency applications poses an existential challenge to conventional cellular networks operating in the sub-6 GHz frequency band. The current sub-6 GHz spectrum for 5G applications represents a short-term solution, where available spectral opportunities are limited and will unquestionably dry up soon. It has driven the evolution of wireless networks toward using millimeter-wave (mmWave) frequencies. MmWave networks offer a range of benefits that make them an attractive choice for 5G and beyond wireless networks [2]. However, the innate challenge of significant pathloss due to high directivity and sensitivity to physical blockages necessitates innovative solutions to ensure reliable and efficient mmWave communication.

Reconfigurable Intelligent Surfaces (RIS) is a software-defined metasurface made up of a large number of tiny, interconnected passive scattering elements which can be electronically controlled to steer the incident waves (by adjusting their phase and amplitude) in a desired direction [3]. RIS have emerged as a promising technology to address the challenges faced by mmWave communication by enabling dynamic manipulation of the wireless propagation environment as they can effectively extend the transmission distance of mmWave communication without requiring additional energy expenditure. Moreover, a RIS has the capability to establish new wireless communication channels by intelligently reflecting the waves around physical blockages. These controllable reflected signals have the added advantage of enhancing physical layer security (PLS) [4]. By adjusting the phase shifts of the reflected signals, the RIS can enhance the desired signal's strength at the desired location while intentionally creating nulls or reducing signal strength at potential eavesdropping locations [5, 6].

RIS-assisted PLS is an emerging field that leverages reflecting surfaces to enhance the security of wireless communication through intelligent control of the wireless propagation environment. This innovative approach holds promise for future secure wireless networks. Initial studies on RIS-assisted PLS have focused on evaluating the secrecy performance of wireless communication in various network settings [7–16]. While works such as [7] and [9] optimize RIS configurations to enhance secrecy rates in a single-user scenario with one potential eavesdropper, they do not consider the impact of multiple users or eavesdroppers. In contrast, [11] extends these efforts to a Multiple-Input Multiple-Output network in the presence of a multi-antenna eavesdropper, proposing metaheuristic solutions for hybrid RIS configurations. Additionally, [10] provides the secrecy outage probability of RIS-assisted Single-Input Single-

A conference version of this work has been accepted for publications in the proc. of IEEE Vehicular Technology Conference (VTC2024-Spring) [1].

This research work is funded by the European Union's Horizon 2020 research and innovation programme under Marie Sklodowska-Curie grant agreement no. 101061011 "RISE-MM" and NATO Science for Peace and Security Programme under grant SPS G5797.

Syed Waqas Haider Shah and Joerg Widmer are with IMDEA Networks Institute, Madrid, Spain. ({syed.waqas, joerg.widmer}@imdea.org).

Marwa Qaraqe is with College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar.

Saud Althunibat is with Department of Communications Engineering, Faculty of Engineering, Al-Hussein Bin Talal University, Maan, Jordan

Output systems but lacks mechanisms for RIS configuration and enhancing secrecy performance. Similarly, [12] explores secrecy performance in a RIS-assisted heterogeneous network by offering a closed-form expression for the asymptotic secrecy outage probability. While these works have established valuable benchmarks for evaluating the secrecy performance of RIS-assisted wireless networks, concerns arise regarding the reliance on perfect channel information for analysis. Moreover, the absence of considerations for the quality-of-service (QoS) guarantees imposed by service providers when studying secrecy performance becomes more critical in the presence of a potential eavesdropper.

In a practical RIS-assisted mmWave system, achieving perfect instantaneous Channel State Information (CSI) poses several intricate challenges [17, 18]. Firstly, wireless signals operating in mmWave frequency bands encounter difficulties in ensuring signal integrity due to higher path loss and susceptibility to atmospheric absorption. Furthermore, the intricate interplay of multipath reflections and beamforming exacerbates the dynamic nature of the channel, leading to beam misalignment and rapid variations in the channel state. These variations are further compounded by the small coherence time in a dynamic RIS-assisted mmWave system with multiple mobile users, adding complexity and resource demands to accurately capture instantaneous channel estimates. Moreover, the BS engages in end-to-end channel estimation, subsequently instructing the RIS to configure reflection coefficients based on the acquired CSI. This process introduces significant delays and complexity. Additionally, in a dynamic multi-user RIS-assisted mmWave network, the CSI received by the BS may become outdated by the time it is processed [19–21]. In summary, due to the swift and unpredictable variations in a RIS-assisted mmWave channel, attempting to maintain up-to-date CSI proves resource-intensive and complex. Therefore, it is imperative to assess the impact of the age of channel information on both the secrecy and QoS performance of the network.

The authors in [22–26] study the impact of imperfect channel estimates on the secrecy performance within a RIS-assisted wireless system. Specifically, [22] presents a solution based on deep reinforcement learning to configure the RIS in the presence of imperfect channel estimates. In a similar vein, [26] formulates a secrecy rate maximization problem, considering a target secrecy rate constraint and optimizing the number of RIS elements while assuming imperfect CSI. The study by [24] investigates the impact of imperfect CSI of eavesdroppers on the secrecy performance in a simultaneous transmission and reflection RIS-assisted non-orthogonal multiple access network. It is noteworthy that the system model in [24] assumes perfect CSI availability for the legitimate node during RIS configuration. In a parallel exploration, [25] focuses on maximizing the secrecy rate of a multicast system. This is achieved through joint optimization of beamforming at the BS and phase shift at the RIS, while acknowledging the imperfect knowledge of the CSI for the wiretap channel. While these works extensively analyze the impact of channel estimation errors in their models, some accounting for wiretap channel errors only, and others considering both legitimate and wiretap channels, they collectively neglect to address the *temporal* aspect of channel estimates - the age of channel information. Investigating the outdatedness of CSI becomes imperative as it underscores the temporal decay of channel information. Furthermore, none of these work, and their referenced literature, investigate the influence of QoS guarantees imposed at the BS on the secrecy performance of the system. This consideration is crucial for any pragmatic scenario, highlighting the need to examine how QoS constraints affect the overall system's secrecy performance.

A. Motivation/Contributions

In pursuit of these objectives, this study aims to optimize the QoS performance within a secure RIS-assisted mmWave network, operating exclusively with outdated channel estimates (for both the wiretap and legitimate channels). The evaluation of QoS performance is conducted by using the effective capacity, an analytical link-layer model [3, 27]. This model takes into account the QoS guarantees imposed at the BS's transmission queue, providing a maximum sustainable constant arrival rate amidst the dynamically changing wireless channel [28]. Specifically, our investigation centers on studying the impact of outdated channel estimates on the joint optimization of transmit beamforming and RIS configuration at the BS and RIS, respectively. The maximum achieved secrecy rate following this joint optimization serves as a benchmark for maximizing the arrival rate at the BS's transmission queue. This maximization is conducted while adhering to the QoS constraints specifically tailored for the secure communication channel under consideration. Moreover, we formulate an optimal transmit power control policy. This policy is designed to maximize the effective secrecy capacity, ensuring both QoS performance and energy-efficient communication. The primary contributions of this paper can be summarized as follows.

- We propose a novel joint optimization mechanism for RIS configuration and transmit beamforming that operates with only the outdated channel estimates while providing the maximum achievable secrecy rate at the legitimate user. The proposed mechanism enables us to investigate the impact of age of channel information on the secrecy capacity of a RIS-assisted mmWave network. Furthermore, we derive a closed-form expression for the noise associated with outdated CSI for both the legitimate user and the eavesdropper channels, revealing its dependency on the age of channel information.
- Next, we present a statistical QoS analysis of the secure RIS-assisted mmWave network. The achieved maximum secrecy rate, resulting from the joint optimization process, serves as a benchmark for maximizing the arrival rate at the BS's transmission queue. This analysis offers a comprehensive examination of the QoS performance within an RIS-assisted mmWave network, taking into account potential eavesdroppers and the impact of aging channel information.
- We propose a novel optimal power control policy designed to maximize the effective secrecy capacity within a secure RIS-assisted mmWave network, even in the

presence of outdated channel estimates. This policy is specifically designed to simultaneously enhance QoS performance and energy efficiency in a secure RIS-assisted mmWave network. Additionally, we find a closed-form solution for the proposed optimal transmit power control policy, allowing for the fine-tuning of system parameters. This fine-tuning not only enhances secrecy and QoS performance but also minimizes the complexity and costs associated with channel estimation, frequent RIS configuration, and energy consumption. The proposed approach represents a significant advancement in optimizing the delicate balance between security, QoS performance, and resource utilization in RIS-assisted mmWave networks.

- Last but not least, we provide a comprehensive evaluation of the proposed schemes through Monte Carlo simulations. The simulation results explore the channel characteristics in near and far-field scenarios, considering various reflective beam patterns and users' velocities. This investigation allows us to understand how a RIS-assisted mmwave channel ages over time in different scenarios. Leveraging these insights, we assess the effectiveness of the proposed joint optimization mechanism for RIS configuration and transmit beamforming, as well as the optimal power control policy, aimed at enhancing the QoS performance in a secure RIS-assisted mmWave network.

B. Paper Outline

The remainder of the paper is organized as follows. Section II presents the system and channel model of a secure RIS-assisted mmWave network. Section III determines the secrecy capacity of the proposed system model under the influence of channel aging (given only outdated channel estimates). Section IV offers a statistical QoS analysis of a secure RIS-assisted mmWave network and introduces an optimal power control policy that maximizes the effective secrecy capacity. Section V presents the performance evaluation of the proposed schemes using Monte-Carlo simulations. Finally, Section VI provides concluding remarks.

C. Notation

The bold lowercase and uppercase represents vectors and matrices, respectively. The symbols $(.)^T$, $(.)^H$, and tr(.) denote the transpose, Hermitian transpose, and trace operators, respectively. The expectation operator is denoted as $\mathbb{E}[.]$, while diag(x) signifies an $n \times n$ diagonal matrix with its diagonal elements corresponding to the elements of vector x. We consider both Rayleigh and Rician fading channels. The Rayleigh fading channel is characterized by a complex fading coefficient h, which follows a complex Gaussian distribution denoted by $\mathcal{CN}(0,1)$, while the power gain $|h|^2$ follows a Rayleigh distribution. The Rician fading channel introduces a Rician factor $\mathcal{R}$, representing the ratio of line-of-sight power to scattered power. The power gain $|h|^2$ in a Rician fading channel follows a Rician distribution.

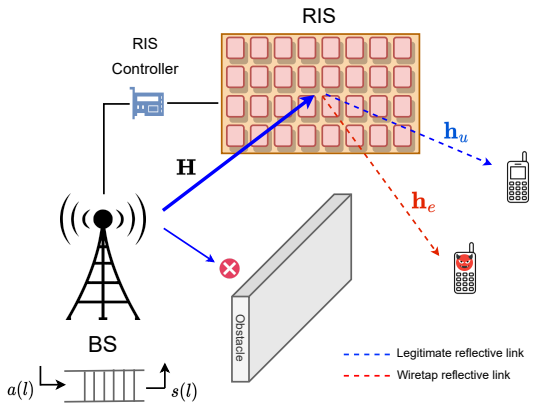

Fig. 1. A secure RIS-assisted mmWave communication network: solid blue arrow represent incident wave, dashed blue arrow and dashed red arrow show reflected waves towards the legitimate user and potential eavesdropper, respectively.

II. System and Channel Model

A. System Model

We consider a RIS-assisted mmWave communication system in which the base station (BS) transmits confidential data to a legitimate user in the presence of a potential eavesdropper, as shown in Fig. 1. In the proposed system model, we leverage a large RIS to increase (decrease) the received signal-to-noise ratio (SINR) at the legitimate user (eavesdropper). The BS and the RIS are equipped with N_B ($b = \{1, 2, \ldots, N_B\}$) transmit antennas and N_R ($r = \{1, 2, \ldots, N_R\}$) reflecting elements, respectively, and the users are single-antenna mobile users. Let $\mathbf{H} \in \mathbb{C}^{N_R \times N_B}$, $\mathbf{h}_u^b \in \mathbb{C}^{1 \times N_B}$, and $\mathbf{h}_e^b \in \mathbb{C}^{1 \times N_B}$ be the channel coefficients of the channel between BS and RIS, RIS and legitimate user, and RIS and potential eavesdropper, respectively [1]. Since we are considering a RIS-assisted mmWave system model in which BS (RIS) performs beamforming towards RIS (legitimate user), all the channels have dominant line-of-sight (LoS) paths. Therefore, $\mathbf{H}$ and $\mathbf{h}_u^b$ channels follow Rician fading, and $\mathbf{h}_e^b$ follows Rayleigh fading. Therefore, by accounting for both line-of-sight (LoS) and non-line-of-sight (NLoS) paths, we can express the channels between BS and the RIS, as well as between the RIS and the legitimate user, as follows.

$$\begin{aligned} \mathbf{H} &= \sqrt{\frac{\mathcal{R}_B}{1+\mathcal{R}_B}}\mathbf{H}^{LoS} + \sqrt{\frac{1}{1+\mathcal{R}_B}}\mathbf{H}^{NLoS} \\ \mathbf{h}_u^b &= \sqrt{\frac{\mathcal{R}_R}{1+\mathcal{R}_R}}\mathbf{h}_u^{LoS} + \sqrt{\frac{1}{1+\mathcal{R}_R}}\mathbf{h}_u^{NLoS}, \end{aligned} \tag{1}$$

[1]This work addresses a secure communication system involving multiple users divided into two groups through an authentication process. Authenticated users are deemed legitimate, while those failing authentication are classified as unrecognized and may eavesdrop on legitimate communications. On the other hand, to counter the risk from fully passive eavesdroppers, one approach is to use adaptive beamforming to create signal nulls throughout the network, except where legitimate users are located. However, this method requires perfect knowledge of communication channels, the environment, RIS configurations, and beam training, which is impractical in real-world situations.

where $\mathcal{R}_B$ and $\mathcal{R}_R$ represent the Rician K-factor. Moreover, we assume that all the channels are block fading channels, in which the channel conditions are assumed to remain relatively constant within each time block and change significantly from one block to the next. These changes can be modeled as independent and identically distributed (i.i.d.) from block to block. The duration of each block depends on the channel coherence time, defined as T. Let $\mathbf{\Omega} \in \mathbb{C}^{N_R \times N_R}$ be the reflection coefficient matrix at the RIS, and can be written as: $\mathbf{\Omega} = \text{diag}[\alpha_1\pi_1, \alpha_2\pi_2, \ldots, \alpha_r\pi_r, \ldots, \alpha_{N_R}\pi_{N_R}]$. Here $\pi_r = e^{j\theta_r}$ is the phase coefficient and α_r is amplitude factor of r^{th} reflecting element of the RIS. The received signal at the legitimate user and the potential eavesdropper become

$$y_u = \sqrt{P_{\text{BS}}}\{\mathbf{h}_u\mathbf{\Omega}\mathbf{H}\}\mathbf{f}s + n_u, \tag{2}$$

and

$$y_e = \sqrt{P_{\text{BS}}}\{\mathbf{h}_e\mathbf{\Omega}\mathbf{H}\}\mathbf{f}s + n_e, \tag{3}$$

respectively, where P_{BS} is the transmit power of the BS, $\mathbf{f}$ is the continuous linear transmit beamforming vector, and n_x for $x = \{u, e\}$ is the complex additive White Gaussian noise (AWGN) with the following distribution: $n_x \sim \mathcal{CN}(0, \sigma_x^2)$.

B. Channel Uncertainty Model (Channel Aging)

In a practical RIS-assisted mmWave system, achieving perfect instantaneous channel estimates presents several complex challenges. It is difficult for wireless signals operating on mmWave frequency bands to ensure signal integrity because of higher pathloss and susceptibility to atmospheric absorption. Moreover, the complicated interplay of multipath reflections and beamforming aggravates the dynamic nature of the channel, causing beam misalignment and prompt variations in the channel state. These variations are further complicated by small coherence time in a dynamic RIS-assisted mmWave system with multiple mobile users, making the task of accurately capturing the instantaneous channel estimates more complex and resource hungry. Furthermore, the BS performs end-to-end channel estimation and then instructs the RIS to configure the reflection coefficients based on the acquired channel estimates, which results in large delays and higher complexity [2]. In short, due to the rapid and unanticipated variations in a RIS-assisted mmWave channel, trying to maintain instantaneous channel estimates can be resource-intensive and complex. Therefore, it becomes important to see how a RIS-assisted mmWave channel ages over time and investigate the relation between actual and outdated channel estimates.

We leverage the following channel uncertainty model for the legitimate channel and the potential eave's channel

$$\mathbf{h}_x = \rho_x\hat{\mathbf{h}}_x + \sqrt{1-\rho_x^2}\mathbf{g}_x, \tag{4}$$

[2]End-to-end channel estimation simplifies the process by estimating the overall channel directly, reducing computational complexity and fitting dynamic environments. However, it lacks the detailed control offered by cascade channel estimation, which provides separate BS-RIS and RIS-user channel information [29]. End-to-end channel estimation is ideal for real-time, rapidly changing conditions, whereas cascade channel estimation is better for stable settings requiring precise control [30].

for $x \in \{u, e\}$. Where $\mathbf{h}_x = \mathbf{h}_x(t+T_{delay})$ denotes the true real-time channel vector at time $(t+T_{delay})$, $\hat{\mathbf{h}}_x = \mathbf{h}_x(t)$ represents the outdated channel vector at time (t), and $\mathbf{g}_x = \hat{\mathbf{h}}_x(t+T_{delay})$ is the estimated real-time channel vector at time $(t+T_{delay})$. Moreover, ρ_x is the correlation strength between the outdated channel vector $\hat{\mathbf{h}}_x$ and the real-time channel vector $\mathbf{h}_x$. The correlation strength depends on the user's velocity (legitimate user and potential eavesdropper) and the Doppler shift due to the user movement. Let v and f^D indicates velocity and maximum Doppler shift, then the correlation strength becomes: $\rho_x = J_0(2\pi f^D\Delta_T)$. Here $\rho_x \approx 1$ ($\rho_x \approx 0$) refers to perfect (zero) correlation between the outdated and instantaneous channel estimates. The received signals in (2) and (3) given the channel uncertainty model become

$$\begin{aligned} y_u^{\text{out}} &= \sqrt{P_{\text{BS}}}\big\{(\rho_u\hat{\mathbf{h}}_u + \sqrt{1-\rho_u^2}\mathbf{g}_u)\mathbf{\Omega}\mathbf{H}\big\}\mathbf{f}s + n_u, \\ &= \underbrace{\sqrt{P_{\text{BS}}}\rho_u\hat{\mathbf{h}}_u\mathbf{\Omega}\mathbf{H}\mathbf{f}s}_{\text{desired signal}} + \underbrace{\sqrt{P_{\text{BS}}(1-\rho_u^2)}\mathbf{g}_u\mathbf{\Omega}\mathbf{H}\mathbf{f}s}_{\text{Channel aging effect}} + n_u \end{aligned} \tag{5}$$

and

$$\begin{aligned} y_e^{\text{out}} &= \sqrt{P_{\text{BS}}}\big\{(\rho_e\hat{\mathbf{h}}_e + \sqrt{1-\rho_e^2}\mathbf{g}_e)\mathbf{\Omega}\mathbf{H}\big\}\mathbf{f}s + n_e, \\ &= \underbrace{\sqrt{P_{\text{BS}}}\rho_e\hat{\mathbf{h}}_e\mathbf{\Omega}\mathbf{H}\mathbf{f}s}_{\text{expected signal}} + \underbrace{\sqrt{P_{\text{BS}}(1-\rho_e^2)}\mathbf{g}_e\mathbf{\Omega}\mathbf{H}\mathbf{f}s}_{\text{Channel aging effect}} + n_e \end{aligned} \tag{6}$$

respectively. In (5), we can observe that if $\rho_u = 1$, the second term (representing the channel aging effect) in the received signal at the legitimate user (y_u^{out}) becomes zero. Consequently, the received signal will consist only of the desired signal (the first term) and the usual thermal noise. However, if $\rho_u < 1$, the second term does not become zero, meaning the received signal is a combination of the desired signal (the first term), the channel aging effect (the second term), and thermal noise. The same applies to the received signal at the potential eavesdropper (y_e^{out}) in (6). Since we know the received signals at legitimate user and potential eavesdropper, we now find the achievable secrecy capacity given the outdated channel estimates. The secrecy capacity can be defined as the difference between the Shannon capacity of the legitimate user and the potential eavesdropper, and for the given system model, is defined as

$$C_s^{\text{out}} = [C_u^{\text{out}} - C_e^{\text{out}}]^+, \tag{7}$$

where $[C_u^{\text{out}} - C_e^{\text{out}}]^+ = \max\{0, [C_u^{\text{out}} - C_e^{\text{out}}]\}$. Further, $C_u^{\text{out}} = B\log_2(1+\gamma_u^{\text{out}})$ and $C_e^{\text{out}} = B\log_2(1+\gamma_e^{\text{out}})$ are the Shannon capacities of the legitimate user and the potential eavesdropper with outdated channel estimates, respectively. By putting these expressions in (7), the secrecy capacity of the said link under outdated channel constraint becomes,

$$C_s^{\text{out}} = B\log_2\left(\frac{1+\gamma_u^{\text{out}}}{1+\gamma_e^{\text{out}}}\right), \tag{8}$$

where B is the allocated bandwidth and γ_u^{out} and γ_e^{out} are the received SNR at legitimate user and eavesdropper, respectively. To find the received SNR, we consider the worst case scenario, in which the impact of age of channel information is

treated as one part of the additive noise. We term that as outdated CSI noise (channel aging effect). Given this, the received SNR can be calculated using the following expressions.

$$\gamma_u^{\text{out}} = \frac{P_{\text{BS}}|\rho_u \hat{\mathbf{h}}_u \mathbf{\Omega}\mathbf{H}|^2\mathbf{f}^2}{P_{\text{BS}}\left|\sqrt{1-\rho_u^2}\mathbf{g}_u\mathbf{\Omega}\mathbf{H}\right|^2\mathbf{f}^2+\sigma_u^2}, \\ \gamma_e^{\text{out}} = \frac{P_{\text{BS}}|\rho_e \hat{\mathbf{h}}_e \mathbf{\Omega}\mathbf{H}|^2\mathbf{f}^2}{P_{\text{BS}}\left|\sqrt{1-\rho_e^2}\mathbf{g}_e\mathbf{\Omega}\mathbf{H}\right|^2\mathbf{f}^2+\sigma_e^2}, \tag{9}$$

where σ_u^2 and σ_e^2 are the variance of the complex AWGN noise of legitimate user's channel and potential eavesdropper's channel, respectively.

After establishing the model for channel uncertainty, which describes the aging process of channels in an mmWave environment, the next section examines how channel aging affects the secrecy capacity of an RIS-assisted mmWave network. Additionally, we propose an alternative beamforming optimization scheme at the BS and the RIS to maximize secrecy capacity and investigate the scheme's sensitivity to channel aging.

III. Secrecy Capacity With Channel Aging

The secrecy capacity is a key performance metric when developing a secure communication system. It guarantees that the communication between the BS and the legitimate user is reliable and confidential, even when potential eavesdroppers in the system aim to thwart the communication. The goal of any secure communication system is to maximize the secrecy capacity, which entails maximum data transmission between legitimate users while preventing potential eavesdroppers from extracting meaningful information. However, as channel estimates age over time, they can significantly compromise the system's secrecy performance by hindering interference mitigation, beamforming effectiveness, resource allocation decisions, and vulnerability to eavesdropping attacks. Therefore, it is imperative to investigate the impact of age of channel information on the secrecy capacity of a RIS-assisted mmWave network.

The maximization of the secrecy capacity C_s^{out} given in (8) is to be achieved through joint optimization of transmit beamforming vector and phase shift matrix at BS and RIS, respectively. By incorporating the received SNR expressions from (9) into (8), the optimization problem at hand becomes

$$\text{(P1)} \quad \max_{\mathbf{f},\mathbf{\Omega}} \quad \log_2\left(\frac{1+(\rho_u^2\widehat{\mathbf{H}}_u^{(1)}\mathbf{f}^2)/\left((1-\rho_u^2)\widehat{\mathbf{H}}_u^{(2)}\mathbf{f}^2+\sigma_u^2\right)}{1+(\rho_e^2\widehat{\mathbf{H}}_e^{(1)}\mathbf{f}^2)/\left((1-\rho_e^2)\widehat{\mathbf{H}}_e^{(2)}\mathbf{f}^2+\sigma_e^2\right)}\right) \\ \text{s.t.} \quad (c_1): \quad \|\mathbf{f}\|^2 \le P_{\text{BS}}, \\ (c_2): \quad |\alpha_r e^{j\theta_r}| = 1, 0 < \theta_r < 2\pi, \forall\, r \in N_R \tag{10}$$

where $\widehat{\mathbf{H}}_u^{(1)} = |\hat{\mathbf{h}}_u\mathbf{\Omega}\mathbf{H}|^2$, $\widehat{\mathbf{H}}_e^{(1)} = |\hat{\mathbf{h}}_e\mathbf{\Omega}\mathbf{H}|^2$, $\widehat{\mathbf{H}}_u^{(2)} = |\mathbf{g}_u\mathbf{\Omega}\mathbf{H}|^2$, and $\widehat{\mathbf{H}}_e^{(2)} = |\mathbf{g}_e\mathbf{\Omega}\mathbf{H}|^2$ are the respective end-to-end channels. The optimization problem in (P1) is NP-hard due to the non-concave objective function with respect to the transmit beamforming vector at BS (constraint c_1) and the reflection coefficient matrix at RIS (constraint c_2). Moreover, the unit modulus constraint imposed on each reflecting cell at the RIS is non-convex. Furthermore, we note that constraints (c_1) and (c_2) are independent of each other, encompassing variables $\mathbf{f}$ and $\alpha_r e^{j\theta_r}$, respectively. This unique feature of the problem (P1) motivates us to solve it through alternating the optimization of these constraints (i.e., first optimize beamforming at BS then optimize beamforming at RIS).

A. Beamforming Optimization at the BS

In this section, our objective is to maximize the problem defined in (P1) by optimizing the transmit beamforming vector ($\mathbf{f}$), while maintaining the reflection coefficient of the RIS elements fixed (fixed $\mathbf{\Omega}$). Let $\sigma_{u,\text{out}}^2 = (1-\rho_u^2)\widehat{\mathbf{H}}_u^{(2)}\mathbf{f}^2$ and $\sigma_{e,\text{out}}^2 = (1-\rho_e^2)\widehat{\mathbf{H}}_e^{(2)}\mathbf{f}^2$, representing the outdated CSI noise effects at the legitimate user and potential eavesdropper, respectively. Subsequently, the optimization problem stated in (P1), expressed in terms of outdated CSI noise, can be reformulated as follows.

$$\text{(P1a)} \quad \max_{\mathbf{f}} \quad \log_2\left(\frac{1+1/(\sigma_{u,\text{out}}^2+\sigma_u^2)\rho_u^2\widehat{\mathbf{H}}_u^{(1)}\mathbf{f}^2}{1+1/(\sigma_{e,\text{out}}^2+\sigma_e^2)\rho_e^2\widehat{\mathbf{H}}_e^{(1)}\mathbf{f}^2}\right), \\ \text{s.t.} \quad \|\mathbf{f}\|^2 \le P_{\text{BS}} \tag{11}$$

The elimination of $\log_2$ from (P1a) is permissible due to its strictly monotonically increasing nature, and $\mathbf{f}^2 = \mathbf{f}^H\mathbf{f}$, where $\mathbf{f}^H$ represent the conjugate transpose of $\mathbf{f}$. Consequently, (P1a) can be further reformulated as:

$$\text{(P1b)} \quad \max_{\mathbf{f}} \quad \frac{1+\rho_u^2/(\sigma_{u,\text{out}}^2+\sigma_u^2)\mathbf{f}^H\widehat{\mathbf{H}}_u^{(1)}\mathbf{f}}{1+\rho_e^2/(\sigma_{e,\text{out}}^2+\sigma_e^2)\mathbf{f}^H\widehat{\mathbf{H}}_e^{(1)}\mathbf{f}}, \\ \text{s.t.} \quad \|\mathbf{f}\|^2 \le P_{\text{BS}} \tag{12}$$

In (P1b), it is noteworthy that the transmit beamforming vector ($\mathbf{f}$) at the BS remains independent of the variables $\widehat{\mathbf{H}}_u^{(1)}$, $\widehat{\mathbf{H}}_e^{(1)}$, and outdated CSI and thermal noise at the legitimate user and potential eavesdropper. Consequently, these elements become constants with respect to $\mathbf{f}$. In light of this, the optimal solution to (P1b) is derived as given in the following [31].

$$\mathbf{f}^{\text{opt}} = \sqrt{P_{\text{BS}}}\lambda_{\max}\left\{\left(\frac{\rho_e^2\widehat{\mathbf{H}}_e^{(1)}}{\sigma_{e,\text{out}}^2+\sigma_e^2}+\frac{I_{N_B}}{P_{\text{BS}}}\right)^{-1}\left(\frac{\rho_u^2\widehat{\mathbf{H}}_u^{(1)}}{\sigma_{u,\text{out}}^2+\sigma_u^2}+\frac{I_{N_B}}{P_{\text{BS}}}\right)\right\}, \tag{13}$$

where I_{N_B} is an identity matrix of size $(N_B \times N_B)$ and $\lambda_{\max}(\mathbf{M})$ is the normalized eigenvector corresponding to the largest eigenvalue of matrix $\mathbf{M}$. It is important to note that the optimal transmit beamforming vector in (13) is influenced by the channel aging process. Therefore, it is essential to assess the impact of channel aging between the BS and the legitimate user, as well as between the BS and the potential eavesdropper, on $\mathbf{f}^{\text{opt}}$. The channel aging process for both channels is determined by the respective channel estimates, which are known to become outdated. For this purpose, Lemma 1 provides closed-form expression for the effect of channel aging process on the legitimate user's channel.

Lemma 1. *The impact of the channel aging process at the legitimate user on the optimal transmit beamforming vector ($\mathbf{f}^{opt}$) can be computed using the following expression.*

$$\sigma_{u,out}^2 = (1-\rho_u^2)(1-\alpha_u^2)\sum_{b=1}^{N_B}|f_b|^2 \tag{14}$$

where α_u is the average value of $\hat{h}_u(t+T_{delay})$.

Proof: Given in Appendix A

Building upon Lemma 1, we obtain the closed-form expression for the noise effect caused by the outdated channel estimates of the legitimate user's channel. Similarly, we can derive a closed-form expression for the impact of the channel aging process on the potential eavesdropper's channel, which is provided by Lemma 2 below.

Lemma 2. *The impact of the channel aging process at the potential eavesdropper on the optimal transmit beamforming vector ($\mathbf{f}^{opt}$) can be computed using the following expression.*

$$\sigma^2_{e,out} = (1-\rho_e^2)(1-\alpha_e^2)\sum_{b=1}^{N_B}|f_b|^2 \tag{15}$$

where α_e is the average value of $\hat{h}_e(t+T_{delay})$.

Proof: Given in Appendix B

Similar to Lemma 1, Lemma 2 presents a closed-form expression detailing the noise effect stemming from outdated channel estimates of the potential eavesdropper's channel. By substituting the final expressions derived in equations (14) and (15) into equation (13), we can determine the optimal transmit beamforming vector at the base station, assuming that the CSI available at the BS is known to be outdated.

Having a solution for problem (P1) with constraint c_1, we then integrate this result back into (P1) and proceed to solve it for c_2. Constraint c_2 specifies that the magnitude of the complex-valued reflection coefficient $e^{j\theta_r}$, associated with a particular phase shift θ_r applied by r^{th} RIS element, must be unity. This condition ensures that, in a lossless environment, the RIS does not introduce additional loss or gain to the signal power but rather adjusts its phase. Thus, constraint c_2 ensures that the RIS elements maintain unit magnitude reflection coefficients, allowing them to manipulate the phase of incident signals effectively without altering their amplitudes.

B. Beamforming Optimization at the RIS

Given the optimal transmit beamforming vector, our goal is to determine the phase shifts of the RIS reflecting elements. [3] This determination is aimed at maximizing the received SNR at the legitimate user while concurrently minimizing the SNR at the potential eavesdropper. In order to optimize the reflection matrix at the RIS, we make the assumption that there exists a direct link between the BS and both the legitimate user and the potential eavesdropper. These direct links serve as a reference to adjust the phase shifts of each reflecting element at the RIS. The assumption of direct links serves as a practical reference point, enabling the optimization process by providing a baseline for comparison. By utilizing the direct links as a benchmark, adjustments to the phase shifts of the RIS elements can be precisely calibrated, ensuring the enhancement of the SNR at the legitimate user and the suppression of the SNR

[3]Note that our proposed beamforming optimization framework primarily focuses on passive RIS due to their energy efficiency and simplicity. However, the proposed framework can be easily extended to accommodate active RIS [32] by incorporating power amplification factors into the optimization problem in (P2).

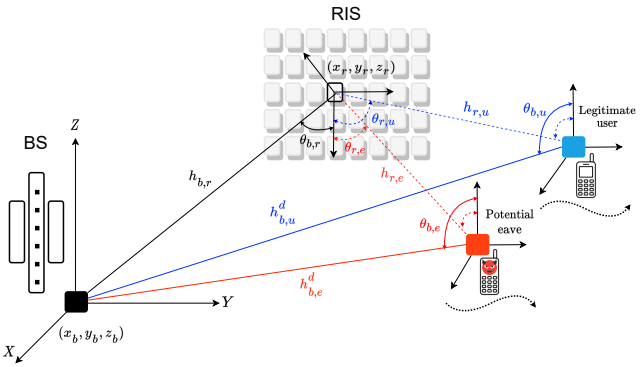

Fig. 2. Polar representation of the direct and RIS-assisted legitimate and wiretap links to the legitimate user and potential eavesdropper, respectively.

at the potential eavesdropper. Consequently, the optimization problem (P1) is reformulated as:

$$\begin{aligned}(\text{P2})\ \max_{\boldsymbol{\Omega}}\ & \log_2\left(\frac{1+1/(\sigma^2_{u,\text{out}}+\sigma^2_u)\left|\rho_u\hat{\mathbf{h}}_u\boldsymbol{\Omega}\mathbf{H}+\rho^d_u\hat{\mathbf{h}}^d_u\right|^2(\mathbf{f}^{\text{opt}})^2}{1+1/(\sigma^2_{e,\text{out}}+\sigma^2_e)\left|\rho_e\hat{\mathbf{h}}_e\boldsymbol{\Omega}\mathbf{H}+\rho^d_e\hat{\mathbf{h}}^d_e\right|^2(\mathbf{f}^{\text{opt}})^2}\right)\\ \text{s.t.}\quad & (c_2):\quad |\alpha_r e^{j\theta_r}|=1,\quad 0<\theta_r<2\pi,\forall_r\in N_R\end{aligned} \tag{16}$$

where $\hat{\mathbf{h}}^d_u$ ($\hat{\mathbf{h}}^d_e$) is a vector that contains the estimated channel coefficients of the direct channel between the BS and the legitimate user (potential eavesdropper), and ρ^d_u and ρ^d_e are the correlation strength of the respective channel. By representing the respective channels in their polar form, as shown in Fig. 2, and after some simplification steps, (16) can be reformulated as given in (17), shown at the top of the next page. In (17), $\hat{h}_{r,u}$ ($\theta_{r,u}$), α_r (θ_r), $h_{b,r}$ ($\theta_{b,r}$), and $\hat{h}^d_{b,u}$ ($\theta_{b,u}$) are the envelope (phase) of the legitimate user's direct and reflected channels, as shown in Fig. 2. Similarly, $\hat{h}_{r,e}$ ($\theta_{r,e}$) and $\hat{h}^d_{b,e}$ ($\theta_{b,e}$) are the envelope (phase) of the potential eavesdropper's direct and reflected channels. The maximization problem in (17) reveals that to maximize the secrecy capacity, the phase shifts of the RIS reflecting elements ($\theta_r, \forall r \in N_R$) should be designed in a way that aligns the phase of the outdated direct channel between the BS and the legitimate user with the phase of the outdated RIS-assisted channel between the BS and the legitimate user. Concurrently, the outdated direct channel between the BS and the potential eavesdropper should be out of phase with the outdated RIS-assisted channel between the BS and the potential eavesdropper.

It is important to note that only the outdated channel estimates are available at the BS to configure the RIS. Therefore, the performance of the phase shifts matrix at the RIS critically depends on the accuracy of the channel estimates. Given the outdated channel estimates, the phase shift of r^{th} reflecting element of the RIS that maximizes (minimizes) the received SINR at the legitimate user (potential eavesdropper) can be calculated

$$\begin{aligned}\theta^*_r &= \arg\max_{0<\theta_r<2\pi}\ \frac{\Gamma^{\text{out}}_u}{(\sigma^2_{u,\text{out}}+\sigma^2_u)} = \left\{\theta_{b,u}-(\theta_{r,u}+\theta_{b,r})\right\}\\ \theta^*_r &= \arg\min_{0<\theta_r<2\pi}\ \frac{\Gamma^{\text{out}}_e}{(\sigma^2_{e,\text{out}}+\sigma^2_e)} = \left\{\theta_{b,e}-(\theta_{r,e}+\theta_{b,r})\right\},\end{aligned} \tag{18}$$

$$\text{(P2a)} \quad \max_{\mathbf{\Omega}} \quad \log_2\left(\frac{1+1/(\sigma^2_{u,\text{out}}+\sigma^2_u)\left|\sum_{b=1}^{N_B}\sum_{r=1}^{N_R}\rho_u\hat{h}_{r,u}\alpha_r h_{b,r}e^{j(\theta_{r,u}+\theta_r+\theta_{b,r})}f_b^{\text{opt}}+\sum_{b=1}^{N_B}\rho_u^d\hat{h}_{b,u}^d e^{j\theta_{b,u}}f_b^{\text{opt}}\right|^2}{1+1/(\sigma^2_{e,\text{out}}+\sigma^2_e)\left|\sum_{b=1}^{N_B}\sum_{r=1}^{N_R}\rho_e\hat{h}_{r,e}\alpha_r h_{b,r}e^{j(\theta_{r,e}+\theta_r+\theta_{b,r})}f_b^{\text{opt}}+\sum_{b=1}^{N_B}\rho_e^d\hat{h}_{b,e}^d e^{j\theta_{b,e}}f_b^{\text{opt}}\right|^2}\right) \tag{17}$$

$$\text{s.t.} \quad (c_2): \quad |\alpha_r e^{j\theta_r}| = 1, \quad 0 < \theta_r < 2\pi, \forall_r \in N_R$$

where $\Gamma_u^{\text{out}} = \left|\sum_{b=1}^{N_B} f_b^{\text{opt}}(\sum_{r=1}^{N_R}\rho_u\hat{h}_{r,u}\alpha_r h_{b,r} + \rho_u^d\hat{h}_{b,u}^d)\right|^2$ and $\Gamma_e^{\text{out}} = \left|\sum_{b=1}^{N_B} f_b^{\text{opt}}(\sum_{r=1}^{N_R}\rho_e\hat{h}_{r,e}\alpha_r h_{b,r} + \rho_e^d\hat{h}_{b,e}^d)\right|^2$. The phase shift in (18) maximizes (minimizes) the received SINR at the legitimate user (potential eavesdropper) under the influence of channel aging effect/ outdated CSI noise (given in Lemma 1). It reveals the relation between the phase shift matrix at the RIS and the degree of correlation between outdated and perfect estimates of the respective channels. As the degree of correlation increases, the performance of the phase shift optimization problem in equation (18) also improves, leading to a higher level of secrecy capacity [4]. However, the correlation strength increases through more frequent estimation of the respective channels, which entails high signaling overhead, especially in the case of RIS-assisted mmWave networks (owing to their extremely large channel matrices). Therefore, finding the right tradeoff between the manageable signaling overhead and the secrecy performance becomes essential in specific system settings.

Given the outdated channel estimates, we aim to determine the impact of imposing statistical QoS guarantees at the BS on the maximum achievable secrecy capacity, referred to as effective secrecy capacity. To achieve this, we utilize Effective Capacity, a link-layer analytical tool that calculates the maximum arrival rate at the finite-sized transmission queue, considering the randomly time-varying channel, while adhering to the QoS constraints specified at the BS.

Remark: *Ideally, both schemes presented in* (18) *should be used together: the phase shift matrix at the RIS should be optimized to maximize the received SINR at the legitimate user while simultaneously minimizing the received SINR at the potential eavesdropper. However, in practice, focusing on maximizing the received SINR at the legitimate user tends to be more effective for enhancing the system's secrecy performance. As a result, most research in the literature prioritizes maximizing the SINR at the legitimate user rather than directly minimizing it at the eavesdropper, since the eavesdropper's SINR will naturally decrease when the legitimate user's SINR is optimized. This approach is particularly effective in mmWave scenarios, where spatial beams with narrower beamwidths are used. Additionally, when designing such systems, it's important to consider the correlation strengths of the channels. If the legitimate user's channel has a strong correlation, the first scheme–focusing on maximizing the legitimate user's SINR – should be favored. On the other hand, if the eavesdropper's channel shows a stronger correlation than the legitimate user's channel, the second scheme – targeting the reduction of the eavesdropper's SINR – might be more effective.:*

[4]When two arriving signals at the legitimate user are completely in-phase, i.e., $(\theta_{r,u}+\theta_r+\theta_{b,r})$ - $\theta_{b,u} = 0$, then the optimal phase shift of r^{th} reflecting element of the RIS is given by: $\theta_r^{\text{opt}} = \theta_{b,u} - (\theta_{r,u}+\theta_{b,r})$. Similarly, when two arriving signals at the potential eavesdropper are completely out of phase, i.e., $(\theta_{r,e}+\theta_r+\theta_{b,r})$ - $\theta_{b,e} = \pi$, they create a null point; consequently, the potential eavesdropper won't be able to intercept the message intended for the legitimate user. In that case, the optimal phase shift of r^{th} reflecting element of the RIS is given by: $\theta_r^{\text{opt}} = \pi + \theta_{b,e} - (\theta_{r,e}+\theta_{b,r})$.

C. Computational Complexity Analysis

The computational complexity of finding the optimal transmit beamforming vector in (13) involves matrix inversion, resulting in a complexity of $O(N_b^3)$, where N_B is the number of transmit antenna elements at the BS. This cubic complexity is typical for operations involving matrix inversion and increases significantly with more BS antennas. Next, according to (18), the computation of the optimal phase shift value for each RIS element r ($r \in \{1, 2, \ldots, N_R\}$) does not involve matrix inversion. Instead, the division by $(\sigma^2_{u,\text{out}}+\sigma^2_u)$ yields a scalar value, and the remaining calculations involve only scalar addition and subtraction. Thus, computing the optimal closed-form solution for a single RIS element requires N_r calculations. Since the RIS consists of N_R reflecting elements, the total computational complexity to determine the optimal RIS phase shift matrix (for all reflecting elements) using the closed-form solution in (18) is $O(N_R^2)$. Therefore, the overall computational complexity of the combined beamforming optimization scheme at both the BS and the RIS is $O(N_b^3)+O(N_R^2) = O(N_B^3+N_R^2)$. Here, note that, the complexity of the proposed optimization scheme would increase with an increase in the number of transmit antenna elements at the BS (N_B) and/or number of reflecting elements at the RIS (N_R).

IV. Statistical QoS Guarantees on Secrecy Capacity

A. Effective Capacity Primer

Effective service capacity in wireless networks refers to the maximum rate at which data can be reliably transmitted and serviced while meeting specific QoS requirements. It is a key metric that accounts for the dynamic nature of wireless environments, including factors such as varying signal strength, channel conditions, network congestion, and bandwidth availability. Unlike traditional capacity metrics that may only consider the physical layer's maximum data rate (e.g., Shannon capacity), effective service capacity integrates the statistical characteristics of service quality, such as delay constraints and packet loss probabilities, ensuring that user demands are met with consistent and acceptable performance levels. By doing so, it provides a more realistic measure of

a network's ability to handle incoming traffic and deliver services efficiently, even under fluctuating network conditions. This concept is particularly important for modern wireless networks, where maintaining high reliability and low latency is crucial for applications ranging from real-time video streaming to mission-critical communications.

From an analytical perspective, effective capacity serves as a tool to determine the maximum continuous data arrival rate that a network can handle at the transmission queue, considering the stochastic nature of wireless channels and the requirement to meet statistical QoS guarantees at the BS's transmission queue. It is defined using the logarithmic moment-generating function (LMGF) of the cumulative service process of the transmission queue, which captures the variability of service and the associated delay constraints [27]. The effective capacity, considering that the BS operates under specific QoS guarantees in terms of delay bounds, is as follows

$$\Pi(\nu) = -\frac{\Lambda(-\nu)}{\nu} = -\lim_{t\to\infty}\frac{1}{\nu t B}\log(\mathbb{E}[e^{-\nu BS(t)}]), \tag{19}$$

where $\Pi(\nu)$ denotes the asymptotic LMGF of the arrival rate at the BS's transmission queue. Here, ν represents the QoS exponent, which defines the statistical QoS requirements, such as delay or outage probability. A higher ν corresponds to stricter QoS requirements, while a lower ν indicates more relaxed QoS constraints. $S(t) = \sum_{l=1}^{t} s(l)$ is the cumulative service process of the channel, dependent solely on the instantaneous channel capacity at time t. As $t \to \infty$, the system approaches a steady-state transmission queue at the BS. Lastly, B is the allocated bandwidth. In conventional wireless communication scenarios, the service process is governed primarily by the Shannon capacity of the channel, which focuses on maximizing the reliable data transmission rate. However, in the context of secure RIS-assisted mmWave networks, security and privacy considerations become paramount.

B. Effective Secrecy Capacity of RIS-Assisted mmWave Networks

In this work, we extend the concept of effective capacity to account for secure communication, introducing the notion of secrecy capacity as a key constraint. In this framework, the service process is not limited solely by the Shannon capacity but is constrained by the system's secrecy capacity, which reflects the ability of the network to maintain information confidentiality and protect against eavesdropping or unauthorized access. Consequently, the effective capacity is modified to accommodate security constraints, with the cumulative service process of the transmission queue at the BS ($S(t)$) represented by the system's secrecy rate ($R_s(t)$). The effective capacity in (19) can be reformulated as the following, which we term as effective secrecy capacity.

$$\Pi(\nu) = -\lim_{t\to\infty}\frac{1}{\nu t B}\log(\mathbb{E}[e^{-\nu B R_s(t)}]), \tag{20}$$

Where $R_s(t)$ represents the instantaneous secrecy rate at time slot t, this rate is influenced by factors like information leakage and decoding error probability. To ensure secure communication, it is essential to set a lower bound on the secrecy rate, accounting for specific levels of information leakage and decoding errors. In wireless communications, information leakage is the probability that an eavesdropper intercepts confidential data, compromising security. Decoding error probability is the chance that the legitimate receiver fails to correctly decode the message, impacting communication reliability. High information leakage forces a lower transmission rate to protect data, while high decoding errors require a reduction in the service rate to maintain reliability. Both factors can decrease the overall secrecy rate. Thus, a lower bound on the instantaneous secrecy rate for a given information leakage (δ) and decoding error probability (ϵ) is expressed as

$$R_s(t) > \begin{cases} C_s(t) - \Omega_u(t) - \Omega_e(t), & \gamma_u^{\text{out}}(t) > \gamma_e^{\text{out}}(t) \\ 0, & \gamma_u^{\text{out}}(t) \le \gamma_e^{\text{out}}(t) \end{cases} \tag{21}$$

where $\Omega_u(t) = \sqrt{\frac{v_u(t)}{T_b}}\frac{Q^{-1}(\epsilon)}{\ln 2}$, $\Omega_e(t) = \sqrt{\frac{v_e(t)}{T_b}}\frac{Q^{-1}(\delta)}{\ln 2}$, and $v_u(t)$ ($v_e(t)$) represents the channel dispersion of the legitimate (wiretap) link, calculated as $v_x(t) = 1 - (1+\gamma_x^{\text{out}}(t))^{-2}$ for $x \in u, e$. Here, Q^{-1} denotes the inverse of the Gaussian Q-function. Moreover, $C_s(t)$ is the maximum achievable secrecy capacity in time slot t, as computed in Section III earlier.

It is important to note that relying solely on outdated channel estimates at the BS can lead to inefficient use of network resources. This inefficiency might cause sub-optimal performance in transmit beamforming at both the BS and the RIS, as well as sub-optimal allocation of transmit power. As a result, these inefficiencies can lead to wasted resources and reduced spectral efficiency, impacting the overall performance of the network. To address this issue, Section III has already introduced an optimal beamforming strategy for both the BS and RIS that considers the impact of outdated channel estimates. Now, we shift our focus to developing an optimal power control policy that aims to maximize the effective secrecy capacity of the RIS-assisted mmWave communication link, given that only outdated channel estimates are available at the BS. To begin, let's define the power control policy specifically tailored for a secure RIS-assisted mmWave network.

C. Power Control Policy

In the secure RIS-assisted mmWave network, the BS adjusts its transmission power based on the knowledge of the channel between the BS and the legitimate user, as well as the eavesdropper. The transmission power adjustment also accounts for the impact of outdated CSI noise, arising due to channel aging. As detailed in Section III, the magnitude squared of the end-to-end channels between the BS and the legitimate user (via RIS) and the BS and the eavesdropper (via RIS) are denoted as $\widehat{\mathbf{H}}_u^{(\text{I})}$ (calculated as $|\hat{\mathbf{h}}_u \boldsymbol{\Omega} \mathbf{H}|^2$) and $\widehat{\mathbf{H}}e^{(\text{I})}$ (calculated as $|\hat{\mathbf{h}}_e \boldsymbol{\Omega} \mathbf{H}|^2$), respectively. Let's define the normalized power control policy as $\Psi(\widehat{\mathbf{H}}_u^{(\text{I})}, \widehat{\mathbf{H}}_e^{(\text{I})}) \triangleq P_{\text{BS}}/\bar{P}_{\text{BS}}$, where $\bar{P}_{\text{BS}}$ is the average maximum transmit power of the BS. Given this, the average transmit power constraint at the BS given the outdated channel estimates is expressed as follows:

$$\mathbb{E}\big[\Psi(\widehat{\mathbf{H}}_u^{(\text{I})}, \widehat{\mathbf{H}}_e^{(\text{I})})\big] = \int_o^\infty \int_o^\infty \Psi(\widehat{\mathbf{H}}_u^{(\text{I})}, \widehat{\mathbf{H}}_e^{(\text{I})}) f_{\widehat{\mathbf{H}}_u^{(\text{I})}}(\widehat{\mathbf{H}}_u^{(\text{I})}) f_{\widehat{\mathbf{H}}_e^{(\text{I})}}(\widehat{\mathbf{H}}_e^{(\text{I})}) \, d_{\widehat{\mathbf{H}}_u^{(\text{I})}} d_{\widehat{\mathbf{H}}_e^{(\text{I})}} \le 1. \tag{22}$$

$$\Pi(\nu) = \frac{-1}{\nu TB}\log\left(\int_o^{\infty}\int_0^{\phi_r\rho_r^2\widehat{\mathbf{H}}_e^{(1)}} f_{\widehat{\mathbf{H}}_u^{(1)}}(\widehat{\mathbf{H}}_u^{(1)}) f_{\widehat{\mathbf{H}}_e^{(1)}}(\widehat{\mathbf{H}}_e^{(1)}) d_{\widehat{\mathbf{H}}_u^{(1)}} d_{\widehat{\mathbf{H}}_e^{(1)}} + \int_o^{\infty}\int_{\phi_r\rho_r^2\widehat{\mathbf{H}}_e^{(1)}}^{\infty} \mathbb{F}[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}),\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}] f_{\widehat{\mathbf{H}}_u^{(1)}}(\widehat{\mathbf{H}}_u^{(1)}) f_{\widehat{\mathbf{H}}_e^{(1)}}(\widehat{\mathbf{H}}_e^{(1)}) d_{\widehat{\mathbf{H}}_u^{(1)}} d_{\widehat{\mathbf{H}}_e^{(1)}}\right).$$
$$\mathbb{F}\big[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}),\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}\big] = \left(\frac{1+\gamma_u^{\text{out}}}{1+\gamma_e^{\text{out}}}\right)^{\frac{-\nu TB}{\ln 2}} . e^{\frac{-\nu TB}{\ln 2}\left(\sqrt{\frac{v_u(t)}{T_b}}Q^{-1}(\epsilon)+\sqrt{\frac{v_e(t)}{T_b}}Q^{-1}(\delta)\right)} \tag{25}$$

Where $f_{\widehat{\mathbf{H}}_u^{(1)}}(\widehat{\mathbf{H}}_u^{(1)})$ and $f_{\widehat{\mathbf{H}}_e^{(1)}}(\widehat{\mathbf{H}}_e^{(1)})$ are the probability distribution function of $\widehat{\mathbf{H}}_u^{(1)}$ and $\widehat{\mathbf{H}}_e^{(1)}$, respectively. Leveraging the power control policy, the received SNR at the legitimate user and the potential eavesdropper in (9) can be reformulated as

$$\gamma_u^{\text{out}} = \frac{\rho_u^2\widehat{\mathbf{H}}_u^{(1)}\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})(\mathbf{f}^{\text{opt}})^2}{(1-\rho_u^2)(1-\alpha_u^2)\sum_{b=1}^{N_B}|f_b^{\text{opt}}|^2\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})+1/\phi_u},$$
$$\gamma_e^{\text{out}} = \frac{\rho_e^2\widehat{\mathbf{H}}_e^{(1)}\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})(\mathbf{f}^{\text{opt}})^2}{(1-\rho_e^2)(1-\alpha_e^2)\sum_{b=1}^{N_B}|f_b^{\text{opt}}|^2\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})+1/\phi_e}, \tag{23}$$

where $\phi_u = \bar{P}_{\text{BS}}/\sigma_u^2$ and $\phi_e = \bar{P}_{\text{BS}}/\sigma_e^2$ are the average SNR at the legitimate user and the potential eavesdropper and $\mathbf{f}^{\text{opt}}$ is the optimal transmit beamforming vector at the BS computed in Section III-A. Moreover, $\mathbb{E}\big[|\sqrt{1-\rho_u^2}\mathbf{g}_u\boldsymbol{\Omega}\mathbf{H}|^2\mathbf{f}^2\big] = (1-\rho_u^2)(1-\alpha_u^2)\sum_{b=1}^{N_B}|f_b^{\text{opt}}|^2$ and $\mathbb{E}\big[|\sqrt{1-\rho_e^2}\mathbf{g}_e\boldsymbol{\Omega}\mathbf{H}|^2\mathbf{f}^2\big] = (1-\rho_e^2)(1-\alpha_e^2)\sum_{b=1}^{N_B}|f_b^{\text{opt}}|^2$ are channel aging effect (outdated CSI noise) at the legitimate user and the potential eavesdropper, respectively. Further details on the calculation of channel aging effect are given in Appendix A and B. Where α_u and α_e are the average values of $\hat{\mathbf{h}}_u(t+T_{delay})$ and $\hat{\mathbf{h}}_e(t+T_{delay})$, respectively. Moreover, f_b^{opt} is the optimal transmit beamforming value for b^{th} transmit antenna, which can be found using (13). Considering the power control policy and the average transmit power constraint, we further explore an optimal power control policy aimed at maximizing the effective secrecy capacity.

D. Optimal Power Control Policy

In this section, our goal is to formulate an optimization problem for the power control policy to achieve the maximum effective secrecy capacity under the influence of channel aging effect (presence of outdated channel estimates). It is noteworthy that $R_s(t) = 0$ when $\gamma_u^{\text{out}} \le \gamma_e^{\text{out}}$, indicating that the secrecy rate is zero ($R_s = 0$) for any power control policy when $\rho_u^2\phi_u\widehat{\mathbf{H}}_u^{(1)}(\mathbf{f}^{\text{opt}})^2 < \rho_e^2\phi_e\widehat{\mathbf{H}}_e^{(1)}(\mathbf{f}^{\text{opt}})^2$. Consequently, the optimal power control policy $\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}) = 0$ within the region $[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})|\rho_u^2\phi_u\widehat{\mathbf{H}}_u^{(1)}(\mathbf{f}^{\text{opt}})^2 < \rho_e^2\phi_e\widehat{\mathbf{H}}e^{(1)}(\mathbf{f}^{\text{opt}})^2]$. Using this, the average transmit power constraint in (22) can be written as

$$\int_o^{\infty}\int_{\phi_r\rho_r^2\widehat{\mathbf{H}}_e^{(1)}}^{\infty}\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}) f_{\widehat{\mathbf{H}}_u^{(1)}}(\widehat{\mathbf{H}}_u^{(1)}) f_{\widehat{\mathbf{H}}_e^{(1)}}(\widehat{\mathbf{H}}_e^{(1)}) d_{\widehat{\mathbf{H}}_u^{(1)}} d_{\widehat{\mathbf{H}}_e^{(1)}} \le 1, \tag{24}$$

where $\phi_r = \phi_e/\phi_u$ represents the ratio between the average SNRs at the potential eavesdropper and the legitimate node, and $\rho_r = \rho_e/\rho_u$ denotes the ratio between the channel correlation strength of the potential eavesdropper link and the legitimate link. Further, by employing the average transmit power constraint in (24), the effective secrecy capacity in (20) can be redefined as presented in (25). The optimal power control policy–aimed at maximizing the effective secrecy capacity while ensuring QoS guarantees and adhering to the average transmit power constraint– can be derived from the following optimization problem.

$$\begin{aligned}(\text{P3}) \quad & \max_{\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})} \Pi(\nu) \\ \text{s.t.} \quad & (c_1): \quad \Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}) \ge 0, \\ & (c_2): \quad \mathbb{E}[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})] \le 1\end{aligned} \tag{26}$$

Here, (P3) aims to find the power control policy that maximizes the effective secrecy capacity. By substituting (25), (P3) can be reformulated as

$$\begin{aligned}(\text{P3a}) \quad & \max_{\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})} \frac{-1}{\nu TB}\log\left(\mathbb{G}_o + \mathbb{G}\big(\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}),\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}\big)\right) \\ \text{s.t.} \quad & (c_1): \quad \Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}) \ge 0, \\ & (c_2): \quad \mathbb{E}[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})] \le 1\end{aligned} \tag{27}$$

where $\mathbb{G}_o = \int_o^{\infty}\int_0^{\phi_r\rho_r^2\widehat{\mathbf{H}}_e^{(1)}} f_{\widehat{\mathbf{H}}_u^{(1)}}(\widehat{\mathbf{H}}_u^{(1)}) f_{\widehat{\mathbf{H}}_e^{(1)}}(\widehat{\mathbf{H}}_e^{(1)}) d_{\widehat{\mathbf{H}}_u^{(1)}} d_{\widehat{\mathbf{H}}_e^{(1)}}$ and

$$\mathbb{G}\big(\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}),\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}\big) = \int_o^{\infty}\int_{\phi_r\rho_r^2\widehat{\mathbf{H}}_e^{(1)}}^{\infty}\mathbb{F}\big[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}),\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}\big] f_{\widehat{\mathbf{H}}_u^{(1)}}(\widehat{\mathbf{H}}_u^{(1)}) f_{\widehat{\mathbf{H}}_e^{(1)}}(\widehat{\mathbf{H}}_e^{(1)}) d_{\widehat{\mathbf{H}}_u^{(1)}} d_{\widehat{\mathbf{H}}_e^{(1)}}.$$

From here, we can observe that $\mathbb{G}_o$ does not change with change in the power control policy; thus, it is independent of the power control policy. Moreover, $\Pi(\nu)$ exhibits a decrease with an increase in $\mathbb{G}\big(\Psi(\widehat{\mathbf{H}}u^{(1)},\widehat{\mathbf{H}}e^{(1)}),\widehat{\mathbf{H}}u^{(1)},\widehat{\mathbf{H}}e^{(1)}\big)$. In other words, maximizing $\Pi(\nu)$ is equivalent to minimizing $\mathbb{G}\big(\Psi(\widehat{\mathbf{H}}u^{(1)},\widehat{\mathbf{H}}e^{(1)}),\widehat{\mathbf{H}}u^{(1)},\widehat{\mathbf{H}}_e^{(1)}\big)$. Consequently, the problem (P3a) in (27) transforms into the following

$$\begin{aligned}(\text{P4}) \quad & \min_{\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})} \mathbb{G}\big(\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}),\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}\big) \\ \text{s.t.} \quad & (c_1): \quad \Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)}) \ge 0, \\ & (c_2): \quad \mathbb{E}[\Psi(\widehat{\mathbf{H}}_u^{(1)},\widehat{\mathbf{H}}_e^{(1)})] \le 1\end{aligned} \tag{28}$$

In problem (P4), it is clear that $\mathbb{G}(.)$ depends on the received SNR at both the legitimate user and the potential eavesdropper. As shown in (23), the received SNR expressions demonstrate that the power control policy significantly affects not only the signal power but also the power of the noise resulting from outdated channel estimates. This dependency creates a highly non-linear and coupled relationship between the power control policy, the signal power, and the noise power, which

complicates the derivation of a general closed-form solution. The interdependence of these factors introduces complex optimization constraints and non-convexity, making it difficult to derive an optimal power control policy analytically. As a result, finding a general solution becomes impractical. To overcome this challenge, we propose focusing on a special case that allows us to simplify the problem and obtain a closed-form solution for the optimization problem outlined in (P4).

E. Special Case for Closed-form Solution

In this section, we investigate a special case that enables us to derive a closed-form solution for the normalized optimal transmit power control policy, which aims to maximize the effective secrecy capacity. We specifically assume that the system operates in a high SNR regime, where $\gamma_x > 15, \mathrm{dB}$. In such high SNR scenarios, it is reasonable to consider the channel dispersion for both the legitimate and eavesdropper channels ($v_u(t)$ and $v_e(t)$) approaching 1. This assumption is based on the observation that the influence of channel dispersion becomes negligible as SNR increases, as demonstrated in [33]. This simplification not only reduces the complexity of the analysis but also provides clearer insights into the impact of the power control policy on the secrecy performance. By substituting the assumption of unity channel dispersion into the secrecy rate expression (21), we can derive a lower bound on the achievable secrecy rate. This lower bound is crucial because it allows us to estimate the minimum performance guaranteed under high SNR conditions. Furthermore, using this lower bound enables us to satisfy Quality of Service (QoS) guarantees more effectively by ensuring that the effective secrecy capacity is maximized under the given power control policy. In summary, focusing on this special case with high SNR and simplified channel dispersion assumptions allows us to derive practical solutions for optimizing secrecy capacity while ensuring QoS requirements are met.

When channel dispersion approaches 1 ($v_x \approx 1$ for $x \in \{u, e\}$), $\mathbb{F}\big(\Psi(\widehat{\mathbf{H}}u^{(\mathrm{l})}, \widehat{\mathbf{H}}e^{(\mathrm{l})}), \widehat{\mathbf{H}}u^{(\mathrm{l})}, \widehat{\mathbf{H}}e^{(\mathrm{l})}\big)$ in (25) becomes

$$\mathbb{F}\big[\Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}), \widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}\big] = \left(\frac{1+\gamma_u^{\mathrm{out}}}{1+\gamma_e^{\mathrm{out}}}\right)^{\frac{-\nu TB}{\ln 2}} \underbrace{e^{\frac{-\nu TB}{\ln 2\sqrt{T_b}}(Q^{-1}(\epsilon)+Q^{-1}(\delta))}}_{\mathrm{a}_1}. \tag{29}$$

In (29), the term (a_1) is constant with respect to the power control policy and does not depend on $\Psi(\widehat{\mathbf{H}}u^{(\mathrm{l})}, \widehat{\mathbf{H}}e^{(\mathrm{l})})$. Thus, by disregarding this constant term, the optimization problem in (P4) can be reformulated as:

$$\begin{aligned} (\mathrm{P4a}) \quad & \min_{\Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})})} \left(\frac{1+\gamma_u^{\mathrm{out}}}{1+\gamma_e^{\mathrm{out}}}\right)^{\frac{-\nu TB}{\ln 2}} f_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}}(\widehat{\mathbf{H}}_u^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}}(\widehat{\mathbf{H}}_e^{(\mathrm{l})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}} \\ \text{s.t.} \quad & (c_1): \quad \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \geq 0, \\ & (c_2): \quad \mathbb{E}[\Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})})] \leq 1 \end{aligned} \tag{30}$$

The optimal solution to (P4a) complies with the requisite necessary first-order constraints, as shown below [34].

$$\begin{aligned} & \frac{\partial \mathbb{J}}{\partial} \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) = 0 \\ & \mathbb{K}\Bigg(\int_0^\infty \int_{\phi_r \rho_r^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})}}^\infty \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}}(\widehat{\mathbf{H}}_u^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}}(\widehat{\mathbf{H}}_e^{(\mathrm{l})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}} - 1 \Bigg) = 0, \\ & \mathbb{K} \geq 0, \quad \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \geq 0, \quad \mathbb{E}[\Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})})] \leq 1 \end{aligned} \tag{31}$$

Where $\mathbb{J}$ and $\mathbb{K}$ are the Lagrangian function and Lagrangian multiplier, respectively. $\mathbb{J}$ can be defined as

$$\begin{aligned} \mathbb{J} = & \int_0^\infty \int_{\phi_r \rho_r^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})}}^\infty \left(\frac{1+\gamma_u^{\mathrm{out}}}{1+\gamma_e^{\mathrm{out}}}\right)^{\frac{-\nu TB}{\ln 2}} f_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}}(\widehat{\mathbf{H}}_u^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}}(\widehat{\mathbf{H}}_e^{(\mathrm{l})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}} + \\ & \mathbb{K}\Bigg(\int_0^\infty \int_{\phi_r \rho_r^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})}}^\infty \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}}(\widehat{\mathbf{H}}_u^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}}(\widehat{\mathbf{H}}_e^{(\mathrm{l})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}} - 1 \Bigg). \end{aligned} \tag{32}$$

In situations where ρ_u and ρ_e approaches 1, indicating nearly perfect correlation strength between outdated and instantaneous channel estimates, the channel aging effect (influence of outdated CSI noise) becomes negligible. By considering $\rho_u \approx 1$ and $\rho_e \approx 1$, the received SNR, as derived from (23), can be expressed as follows

$$\begin{aligned} \gamma_u^{\mathrm{out}} &= \rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_u \\ \gamma_e^{\mathrm{out}} &= \rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_e \end{aligned} \tag{33}$$

Substituting the updated SNR values from (33) into (32), we can rewrite it as presented in (34) at the top of the next page. The computation of the partial derivative of the Lagrangian function, as defined in (34), with respect to the normalized power control policy is expressed as follows.

$$= \frac{\partial}{\partial \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})})} \Bigg\{ \left(\frac{1+\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_u}{1+\rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_e} \right)^{\frac{-\nu TB}{\ln 2}} + \mathbb{K} \Bigg\} f_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}}(\widehat{\mathbf{H}}_u^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}}(\widehat{\mathbf{H}}_e^{(\mathrm{l})}). \tag{35}$$

The final term after the computation of partial derivative comes out to be the following

$$= \Bigg\{ \mathbb{K} - \frac{\mho_1 \times \left(\frac{1+\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_u}{1+\rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_e} \right)^{\frac{\ln 2 - \nu TB}{\ln 2}}}{\left(1 + \rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{l})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{l})}, \widehat{\mathbf{H}}_e^{(\mathrm{l})}) \phi_u\right)^2} \Bigg\} f_{\widehat{\mathbf{H}}_u^{(\mathrm{l})}}(\widehat{\mathbf{H}}_u^{(\mathrm{l})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{l})}}(\widehat{\mathbf{H}}_e^{(\mathrm{l})}), \tag{36}$$

where $\mho_1 = \left\{ \nu TB (\mathbf{f}^{\mathrm{opt}})^2 (\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{l})} \phi_u - \rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{l})} \phi_e) \right\} / \ln 2$. To meet specific QoS requirements within a predetermined block length for a block fading channel, it is imperative to dynamically adapt the available bandwidth for transmission. The derivation of a closed-form solution involves meticulous adjustment of the bandwidth to align with the QoS constraints imposed on the transmission queue and the channel's coherence time. To obtain this closed-form solution, we parameterize the bandwidth as $B = \frac{\ln 2}{\nu T}$. Upon substituting this expression into (31), the resulting streamlined expression for

$$\mathbb{J} = \int_0^\infty \int_{\phi_r \rho_r^2 \widehat{\mathbf{H}}_e^{(\mathrm{I})}}^\infty \left(\frac{1+\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{I})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{I})}, \widehat{\mathbf{H}}_e^{(\mathrm{I})}) \phi_u}{1+\rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{I})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{I})}, \widehat{\mathbf{H}}_e^{(\mathrm{I})}) \phi_e} \right)^{\frac{-\nu T B}{\ln 2}} f_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}}(\widehat{\mathbf{H}}_u^{(\mathrm{I})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}}(\widehat{\mathbf{H}}_e^{(\mathrm{I})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}} + \mathbb{K} \left(\int_0^\infty \int_{\phi_r \rho_r^2 \widehat{\mathbf{H}}_e^{(\mathrm{I})}}^\infty \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{I})}, \widehat{\mathbf{H}}_e^{(\mathrm{I})}) f_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}}(\widehat{\mathbf{H}}_u^{(\mathrm{I})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}}(\widehat{\mathbf{H}}_e^{(\mathrm{I})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}} - 1 \right). \tag{34}$$

the partial derivative of the Lagrangian function, as delineated in (36), is presented below:

$$\left\{ \mathbb{K} - \frac{(\mathbf{f}^{\mathrm{opt}})^2 (\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{I})} \phi_u - \rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{I})} \phi_e)}{\left(1+\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{I})} (\mathbf{f}^{\mathrm{opt}})^2 \Psi(\widehat{\mathbf{H}}_u^{(\mathrm{I})}, \widehat{\mathbf{H}}_e^{(\mathrm{I})}) \phi_u\right)^2} \right\} f_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}}(\widehat{\mathbf{H}}_u^{(\mathrm{I})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}}(\widehat{\mathbf{H}}_e^{(\mathrm{I})}) = 0. \tag{37}$$

The optimal solution is required to adhere to (37) across all values of $\widehat{\mathbf{H}}_u^{(\mathrm{I})}$ and $\widehat{\mathbf{H}}_e^{(\mathrm{I})}$. Consequently, it follows that $\mathbb{K} > 0$, and the derivation of the closed-form expression for the optimal solution is outlined below.

$$\Psi^{\mathrm{opt}}_{B=\frac{\ln 2}{\nu T}}(\widehat{\mathbf{H}}_u^{(\mathrm{I})}, \widehat{\mathbf{H}}_e^{(\mathrm{I})}) = \begin{cases} \frac{\mho_2}{\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{I})} (\mathbf{f}^{\mathrm{opt}})^2 \phi_u}, & \widehat{\mathbf{H}}_u^{(\mathrm{I})} - \frac{\phi_e \rho_e^2}{\phi_u \rho_u^2} \widehat{\mathbf{H}}_e^{(\mathrm{I})} > \frac{\mathbb{K}}{\phi_u} \\ 0, & \widehat{\mathbf{H}}_u^{(\mathrm{I})} - \frac{\phi_e \rho_e^2}{\phi_u \rho_u^2} \widehat{\mathbf{H}}_e^{(\mathrm{I})} \leq \frac{\mathbb{K}}{\phi_u} \end{cases} \tag{38}$$

where $\mho_2 = \sqrt{\frac{(\mathbf{f}^{\mathrm{opt}})^2 (\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{I})} \phi_u - \rho_e^2 \widehat{\mathbf{H}}_e^{(\mathrm{I})} \phi_e)}{\mathbb{K}}} - 1$. The optimal power control policy employs a water-filling strategy, and the determination of the value of $\mathbb{K}$ is essential to ensure compliance with the average transmit power constraint, as described below. This constraint is derived by substituting (38) into (31).

$$\int_0^\infty \int_{\frac{\phi_e \rho_e^2}{\phi_u \rho_u^2} \widehat{\mathbf{H}}_e^{(\mathrm{I})} + \frac{\mathbb{K}}{\phi_u}}^\infty \frac{\mho_2}{\rho_u^2 \widehat{\mathbf{H}}_u^{(\mathrm{I})} (\mathbf{f}^{\mathrm{opt}})^2 \phi_u} f_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}}(\widehat{\mathbf{H}}_u^{(\mathrm{I})}) f_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}}(\widehat{\mathbf{H}}_e^{(\mathrm{I})}) d_{\widehat{\mathbf{H}}_u^{(\mathrm{I})}} d_{\widehat{\mathbf{H}}_e^{(\mathrm{I})}} = 1. \tag{39}$$

In this context, it is noteworthy that $\frac{\phi_e \rho_e^2}{\phi_u \rho_u^2} \widehat{\mathbf{H}}_e^{(\mathrm{I})} + \frac{\mathbb{K}}{\phi_u}$ is a monotonically increasing function of $\mathbb{K}$, and $\mho_2$ is likewise a monotonically decreasing function of $\mathbb{K}$. Consequently, (39) evolves into a monotonically decreasing function with respect to $\mathbb{K}$. As a result, the value of $\mathbb{K}$ that satisfies (39) is unique and can be determined through binary search, denoted as $\mathbb{K}^{\mathrm{opt}}$.

The problem for the special case ($B = \frac{\ln 2}{\nu T}$ and $v_x \approx 1$) is convex. Consequently, the closed-form solution derived in this section is globally optimal. It is pertinent to emphasize that this closed-form solution serves as an upper bound for the achievable effective secrecy capacity, given our assumption of $\rho_x \approx 1$ (indicating a very good correlation strength between instantaneous and outdated channel estimates). In the simulation section, we will explore the impact of the channel aging (outdated CSI noise) on the achievable effective secrecy capacity. We aim to elucidate the extent of effective secrecy capacity loss as the channel ages.

V. Performance Evaluation

This section evaluates the analytical findings of this paper through Monte Carlo simulations and discusses the valuable insights derived from these simulation results.

A. Simulation Setup

In our simulation environment, a multi-antenna BS establishes communication with a legitimate node through a RIS integrated into the network, while contending with the potential presence of eavesdroppers, as illustrated in Fig. 3. The BS deploys a uniform linear array with a size of $N_B = 32$, and the RIS is configured as a rectangular array with dimensions $N_R = 64 \times 64$ (unless stated otherwise). The antenna (reflecting) element spacing at the BS (RIS) is set to $\lambda/2$. All channels exhibit Rayleigh fading, with the link from BS to RIS to the legitimate user incorporating Rician fading due to the presence of a robust line-of-sight component. The channel models are characterized using the IEEE 802.11ay multipath fading channel model, employing a quasi-deterministic approach. Our system adheres to the IEEE 802.11ay standard and utilizes a codebook of beam patterns for beam training at the RIS. We follow the beam pattern generation approach outlined in [19, 35], allowing for the creation of beam patterns with varying beam widths. Additionally, for an RIS with 128 beam patterns, the time required to configure the RIS-assisted link is 5.3 milliseconds, as specified by the IEEE 802.11ay standard [36]. We design the channel models for RIS-assisted mmWave network in near-field and far-field using the model presented in [37]. The carrier frequency is set at $f_c = 28GHz$, and the noise floor is established at $-60dBm$.

B. Simulation Results

This section presents the simulation results and their discussion.

Fig. 4 investigates the characteristics of a RIS-assisted mmWave legitimate channel in near-field and far-field scenarios, considering different beam patterns at the RIS and varying user velocities. In Fig. 4(a), it is observed that the channel ages more rapidly when the user is positioned in the near-field of the RIS compared to the far-field. It is because, with a certain user velocity and beamwidth, the probability of coverage outage is higher in the near field. Moreover, Fig. 4(a) illustrates that the channel aging process can be decelerated by utilizing a wider beam pattern at the RIS. However, this strategy comes at the cost of reduced received signal strength at the legitimate user. A similar phenomenon is also observed in Fig. 4(b), where the channel correlation strength decreases exponentially fast with higher user mobility in the near-field of the RIS. The results presented in this figure contribute to a comprehensive understanding of the time-varying nature of RIS-assisted mmWave communication channels under various operational conditions. The figure provides valuable insights into how a RIS-assisted mmWave channel ages over time and underscores the factors that directly influence the channel

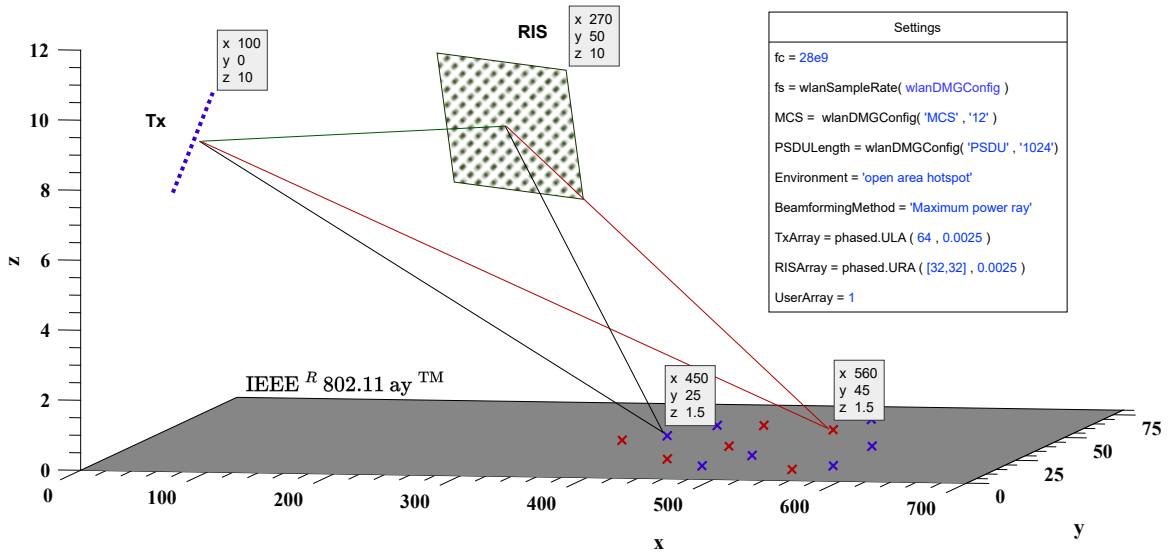

Fig. 3. A 3D representation of the simulation environment of a RIS-assisted mmWave communication network: blue and red cross represent the legitimate user and potential eavesdropper, respectively.

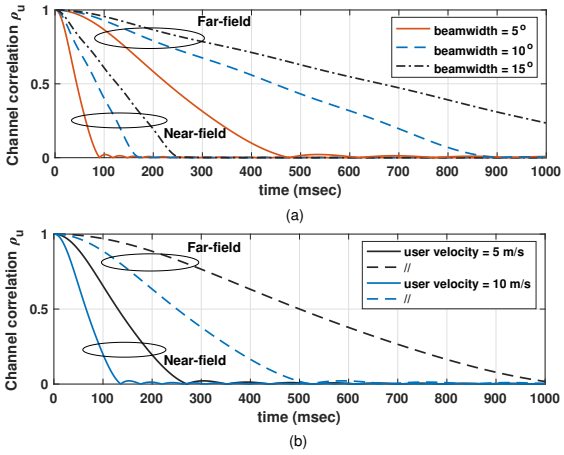

Fig. 4. Age of channel information of a RIS-assisted mmWave link over time with user mobility in near-field and far-field of the RIS; (a) correlation strength for different beam widths, (b) correlation strength for different user velocity.

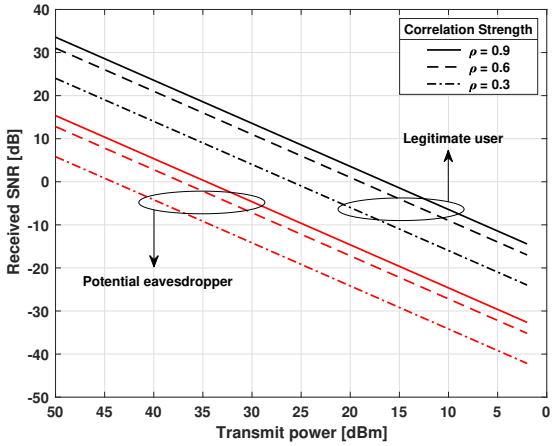

Fig. 5. Impact of the transmit power of the BS on the received SNR at the legitimate user and potential eavesdropper for different correlation strength between the perfect and outdated channels.

aging process. Furthermore, this knowledge is leveraged to optimize beamforming at both the BS and the RIS.

In Fig. 5, we investigate the influence of the BS's transmit power on the received SNR for both the legitimate user and a potential eavesdropper, considering varying correlation strength between perfect and outdated channel information. As expected, we observe that the received SNR linearly decreases with a reduction in transmit power. Furthermore, we notice that the ratio between the received SNR at the legitimate node and the potential eavesdropper remains constant with a decrease in transmit power, as long as the received SNR at the eavesdropper remains above the noise floor. The moment the received SNR at the eavesdropper falls below the noise floor, the impact of the wiretap channel (the channel between the BS and the potential eavesdropper) on the secrecy capacity of the legitimate channel becomes negligible. At that point, the only factors influencing the secrecy capacity are the received SNR at the legitimate user and the thermal noise (and interference, if present). Additionally, this figure highlights the influence of correlation strength on the received SNR. When the channel information is outdated, the RIS configuration is suboptimal, and the transmit power control policy is also affected by the outdated CSI noise, resulting in a loss in received SNR.

The relationship between secrecy capacity and transmit power in an RIS-assisted mmWave channel is fundamental to the secrecy performance of the communication link. As transmit power increases, the potential for secure communication typically improves, given that a stronger signal can be received by the legitimate user. However, this relationship is nuanced, as

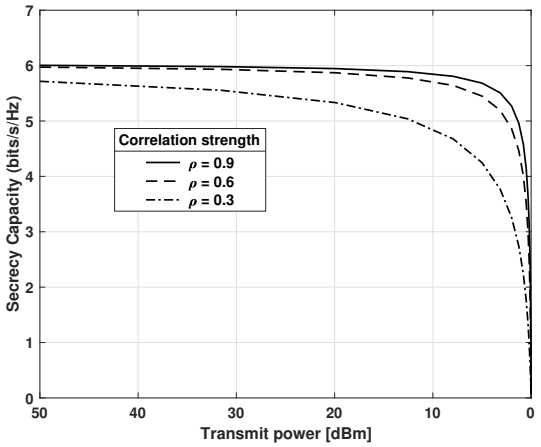

Fig. 6. Secrecy capacity as a function of the transmit power of the BS for different correlation strength between the perfect and outdated channels.

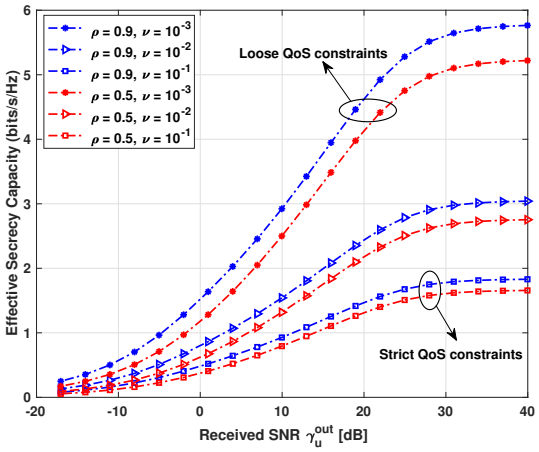

Fig. 8. Impact of the received SNR at the legitimate user on the effective secrecy capacity varies with the age of channel information and the statistical QoS guarantees imposed at the BS.

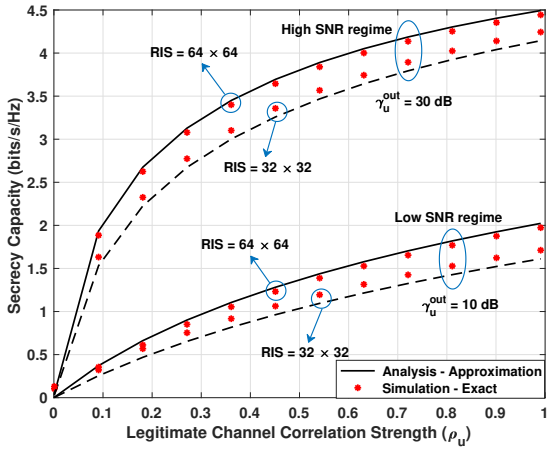

Fig. 7. Impact of channel correlation strength on secrecy performance: secrecy capacity vs legitimate channel correlation strength for different RIS size and SNR regimes.

excessive power may increase the risk of eavesdropping, compromising the confidentiality of the communication. Striking a balance between sufficient power for reliable communication and avoiding unnecessary exposure to potential eavesdroppers is crucial for optimizing the secrecy capacity of a wireless channel. To this end, Fig. 6 leverages the results shown in Fig. 5 and investigates the impact of varying transmit power on the secrecy capacity of the RIS-assisted mmWave link. We observe that the secrecy capacity remains almost constant (6 bits/s/Hz) when the BS's transmit power decreases from 50 dBm to 5 dBm for strong channel correlation strength. A further decrease in transmit power shows an exponential drop in achievable secrecy capacity. This result emphasizes that an unnecessary increase in transmit power does not necessarily improve the secrecy capacity of the RIS-assisted mmWave link, underscoring the importance of optimal transmit power management strategies in an RIS-assisted mmWave system to ensure both reliable and secure information transmission.

Fig. 7 shows that a strong correlation between perfect and outdated estimates of the legitimate user's channel leads to improved secrecy capacity. It is because the legitimate user's channel information is utilized to configure the RIS, and a higher correlation strength facilitates the attainment of an optimal RIS configuration, thereby resulting in enhanced secrecy capacity. It is also important to note that the proposed beamforming design provides adequate secrecy capacity even with weak correlation strength ($0.4 < \rho_u < 0.8$) in a high SNR regime. It demonstrates that infrequent RIS configuration, even with outdated CSI, can still deliver satisfactory secrecy performance. This, in turn, reduces the high signaling overhead and complexity associated with frequent channel estimation and RIS configuration. Additionally, this figure also shows that the proposed beamforming design performs better with a larger RIS (64×64), ultimately achieving higher secrecy capacity. Last but not least, we observe a pronounced influence of channel correlation strength on secrecy capacity in the high SNR regime, as opposed to the low SNR regime.

Next, we explore the effective secrecy capacity given the statistical QoS guarantees imposed on the transmission queue, taking into account the optimal transmit power policy outlined in (38). To this end, Fig. 8 shows that as more stringent QoS constraints are applied at the BS, the increase in effective secrecy capacity with rising SNR at the legitimate user becomes constrained. This issue arises due to the fact that when there are stricter quality of service (QoS) requirements, there is a higher chance of packet loss during wireless transmission because of the unpredictability of the communication channel and the need for enhanced QoS assurances. As a result, there is an increase in packet retransmissions, which depends on the retransmission framework used, thereby limiting the number of unique packets that can be managed in the transmission queue. This consequently leads to a reduction in the effective secrecy capacity. On the other hand, when there are looser QoS restrictions, the transmission queue at the base station (BS) can handle a larger number of unique packets, resulting in a signif-

icantly improved effective secrecy capacity. Furthermore, the results in Fig. 8 indicates that using the proposed beamforming techniques at the BS and the RIS (given in (13) and (18), respectively), coupled with the optimal transmit power policy (given in (38)), yields nearly identical secrecy performance under both weak channel correlation ($\rho_u = 0.5$) and strong channel correlation ($\rho_u = 0.9$). This finding underscores the effectiveness of the proposed techniques in practical scenarios where achieving perfect instantaneous channel estimates is either impossible or impractical due to the high signaling overhead and complexity associated with frequent channel estimation.

VI. Conclusion

We investigated the impact of the age of channel information on the QoS performance of a secure RIS-assisted mmWave network. The performance of any RIS-assisted mmWave system critically depends on the quality and age of channel estimates, and it degrades as the channel estimates become outdated. To address this issue, we proposed a technique for the joint optimization of transmit beamforming and RIS configuration, accompanied by an optimal transmit power control policy. Notably, our approach assesses the actual impact of the age of channel information on the QoS performance of a secure RIS-assisted mmWave network, representing a novel contribution to the field. Our Monte Carlo simulations reveal that utilizing the proposed beamforming techniques at the BS and the RIS, along with the optimal transmit power policy, results in nearly identical secrecy performance under both weak channel correlation and strong channel correlation. This finding underscores the effectiveness of the proposed techniques in practical scenarios where achieving perfect instantaneous channel estimates is either impossible or impractical due to the high signaling overhead and complexity associated with frequent channel estimation. It allows for the tuning of system parameters to ensure enhanced secrecy and QoS performance while minimizing the complexity and costs associated with channel estimation and frequent RIS configuration.

In summary, this work contributes to the evolving landscape of secure mmWave communication by providing practical solutions for RIS optimization under real-world constraints. As we navigate the dynamic interplay between channel aging and system performance, our work establishes a foundation for more energy-efficient, secure, and sustainable RIS-assisted mmWave networks.

Appendix A

The channel aging effect (outdated CSI noise) at the legitimate user is

$$\sigma^2_{u,\text{out}} = (1-\rho_u^2)\mathbb{E}\big[|\mathbf{g}_u\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big], \tag{40}$$

where $\mathbb{E}\big[|\mathbf{g}_u\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big]$ represents the expected value of the square of the magnitude of the end-to-end channel between the BS and the legitimate user through RIS. It can be solved as the following [38]

$$\mathbb{E}\big[|\mathbf{g}_u\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big] = \mathbb{E}\bigg[\bigg|\sum_{r=1}^{N_R}\sum_{b=1}^{N_B} g_{u,r}h_{r,b}e^{j\theta_r}f_b\bigg|^2\bigg], \tag{41}$$

where $\mathbf{g}_u = \{g_{u,1}, g_{u,2}, \ldots, g_{u,r}, \ldots, g_{u,N_R}\}$ and $h_{r,b}$ for $r \in \{1,2,\ldots,N_R\}$ and $b \in \{1,2,\ldots,N_B\}$. Further, it becomes

$$\begin{aligned}\mathbb{E}\big[|\mathbf{g}_u\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big] &= \mathbb{E}\bigg[\bigg|\sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\sum_{l=1}^{N_R}\sum_{c=1}^{N_B} g_{u,r}h_{r,b}e^{j\theta_r}f_b g^*_{x,l}h^*_{l,c}e^{-j\theta_l}f_c\bigg|\bigg] \\ &= \underbrace{\sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\mathbb{E}\Big[\big|g_{u,r}\big|^2\big|h_{r,b}\big|^2\big|f_b\big|^2\Big]}_{\text{a}_1} + \\ &\quad \underbrace{\sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\sum_{l=1,l\neq r}^{N_R}\sum_{c=1,c\neq b}^{N_B}\mathbb{E}\big[g_{u,r}h_{r,b}g^*_{u,l}h^*_{l,c}f_bf_c\big]e^{j(\theta_l-\theta_r)}}_{\text{a}_2}.\end{aligned} \tag{42}$$

Since the channel coefficients $\mathbf{g}_u$ and $\mathbf{H}$ are not related to each other and $\mathbb{E}[g_{u,r}] = 0$. Consequently, a_2 equals zero. Additionally, $h_{r,b} \sim \mathcal{CN}(0,1)$ and $\mathbb{E}\big[\big|g_{u,r}\big|^2\big] = \sigma^2_{\hat{h}_u(t+T_{delay})} = 1-\alpha_u^2$, where α_u is the average value of $\hat{h}_u(t+T_{delay})$. Consequently, we have the following

$$\begin{aligned}\mathbb{E}\big[|\mathbf{g}_u\mathbf{\Omega}\mathbf{H}|^2\big] &= \sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\mathbb{E}\big[\big|g_{u,r}\big|^2\big]\mathbb{E}\big[\big|h_{r,b}\big|^2\big|f_b\big|^2\big] \\ &= \sum_{n=1}^{N_R}\sum_{b=1}^{N_B}\sigma^2_{\hat{h}_{u,r}(t+T_{delay})}\Big(\sigma^2_{h_{r,b}} + \mathbb{E}\big[|h_{r,b}|\big]^2\Big)\big|f_b\big|^2 \\ &= (1-\alpha_u^2)\sum_{b=1}^{N_B}\big|f_b\big|^2.\end{aligned} \tag{43}$$

By substituting this value, the final term for the channel aging effect (outdated CSI noise) at the legitimate user becomes

$$\sigma^2_{u,\text{out}} = (1-\rho_u^2)(1-\alpha_u^2)\sum_{b=1}^{N_B}\big|f_b\big|^2. \tag{44}$$

From this point, it becomes evident that to find the channel aging effect at the legitimate user, we require total energy of the transmit beamforming scheme, the correlation coefficient between outdated and perfect channel estimates of the legitimate user's channel, and the average value of the estimated channel response between the RIS and the legitimate user's channel at time $(t + T_{\text{delay}})$.

Appendix B

The channel aging effect (outdated CSI noise) at the potential eavesdropper is

$$\sigma^2_{e,\text{out}} = (1-\rho_e^2)\mathbb{E}\big[|\mathbf{g}_e\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big], \tag{45}$$

where $\mathbb{E}\big[|\mathbf{g}_e\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big]$ represents the expected value of the square of the magnitude of the end-to-end channel between the BS and the potential eavesdropper through RIS [5]. It can

[5]In the case of an end-to-end eavesdropping channel, the BS can rely on either partial or full channel information. Partial channel information entails limited information at the BS, such as path loss and channel gains. Conversely, full channel information includes detailed parameters like channel gains, phase shifts, and fading statistics. With full channel information, precise control over transmit beamforming and RIS reflection properties is possible, leading to enhanced performance in capacity, coverage, and security. However, even with partial channel information, significant improvements are attainable through adaptive algorithms and optimization techniques tailored to the available channel knowledge.

be solved as the following [38]

$$\mathbb{E}\big[|\mathbf{g}_e\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big] = \mathbb{E}\Bigg[\Bigg|\sum_{r=1}^{N_R}\sum_{b=1}^{N_B} g_{e,r}h_{r,b}e^{j\theta_r}f_b\Bigg|^2\Bigg], \tag{46}$$

where $\mathbf{g}_e = \{g_{e,1}, g_{e,2}, \ldots, g_{e,r}, \ldots, g_{e,N_R}\}$ and $h_{r,b}$ for $r \in \{1,2,\ldots,N_R\}$ and $b \in \{1,2,\ldots,N_B\}$. Further, it becomes

$$\begin{aligned}\mathbb{E}\big[|\mathbf{g}_e\mathbf{\Omega}\mathbf{H}\mathbf{f}|^2\big] &= \mathbb{E}\Bigg[\Bigg|\sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\sum_{l=1}^{N_R}\sum_{c=1}^{N_B} g_{e,r}h_{r,b}e^{j\theta_r}f_b g^*_{e,l}h^*_{l,c}e^{-j\theta_l}f_c\Bigg|\Bigg] \\ &= \underbrace{\sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\mathbb{E}\Big[|g_{e,r}|^2|h_{r,b}|^2|f_b|^2\Big]}_{\mathrm{a}_1} + \\ &\underbrace{\sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\sum_{l=1,l\neq r}^{N_R}\sum_{c=1,c\neq b}^{N_B}\mathbb{E}\big[g_{e,r}h_{r,b}g^*_{e,l}h^*_{l,c}f_bf_c\big]e^{j(\theta_l-\theta_r)}}_{\mathrm{a}_2}.\end{aligned} \tag{47}$$

Since the channel coefficients $\mathbf{g}_e$ and $\mathbf{H}$ are not related to each other and $\mathbb{E}[g_{e,r}] = 0$. Consequently, a_2 equals zero. Additionally, $h_{r,b} \sim \mathcal{CN}(0,1)$ and $\mathbb{E}\big[|g_{e,r}|^2\big] = \sigma^2_{\hat{h}_e(t+T_{delay})} = 1-\alpha_e^2$, where α_e is the average value of $\hat{h}_e(t+T_{delay})$.. Consequently, we have the following

$$\begin{aligned}\mathbb{E}\big[|\mathbf{g}_e\mathbf{\Omega}\mathbf{H}|^2\big] &= \sum_{r=1}^{N_R}\sum_{b=1}^{N_B}\mathbb{E}\big[|g_{e,r}|^2\big]\mathbb{E}\big[|h_{r,b}|^2|f_b|^2\big] \\ &= \sum_{n=1}^{N_R}\sum_{b=1}^{N_B}\sigma^2_{\hat{h}_{e,r}(t+T_{delay})}\big(\sigma^2_{h_{r,b}} + \mathbb{E}\big[|h_{r,b}|\big]^2\big)|f_b|^2 \\ &= (1-\alpha_e^2)\sum_{b=1}^{N_B}|f_b|^2.\end{aligned} \tag{48}$$

By substituting this value, the final term for the channel aging effect (outdated CSI noise) at the legitimate user becomes

$$\sigma^2_{u,\text{out}} = (1-\rho_e^2)(1-\alpha_e^2)\sum_{b=1}^{N_B}|f_b|^2. \tag{49}$$

Similar to Lemma 1, in order to find the channel aging effect at the potential eavesdropper, we need total energy of the transmit beamforming scheme, the correlation coefficient between outdated and perfect channel estimates of the potential eavesdropper's channel, and the average value of the estimated channel response between the RIS and the potential eavesdropper's channel at time $(t+T_{\text{delay}})$.

REFERENCES

[1] S. W. H. Shah, M. Qaraqe, S. Althuniabat, and J. Widmer, "On the impact of age of channel information on secure ris-assisted mmwave networks," in *Proc. IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, 2024, pp. 1–10.

[2] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter wave communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[3] S. W. H. Shah, A. N. Mian, S. Mumtaz, A. Al-Dulaimi, I. Chih-Lin, and J. Crowcroft, "Statistical QoS analysis of reconfigurable intelligent surface-assisted D2D communication," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7343–7358, 2022.

[4] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electronics*, vol. 4, no. 11, pp. 827–836, 2021.

[5] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[6] S. Keşir, S. Kayraklık, İ. Hökelek, A. E. Pusane, E. Basar, and A. Görçin, "Measurement-based characterization of physical layer security for RIS-assisted wireless systems," in *Proc. IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 2023, pp. 1–6.

[7] K. Feng, X. Li, Y. Han, S. Jin, and Y. Chen, "Physical layer security enhancement exploiting intelligent reflecting surface," *IEEE Communications Letters*, vol. 25, no. 3, pp. 734–738, 2020.

[8] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2637–2652, 2020.

[9] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[10] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 296–12 300, 2020.

[11] E. N. Egashira, D. P. M. Osorio, N. T. Nguyen, and M. Juntti, "Secrecy capacity maximization for a hybrid relay-RIS scheme in mmwave MIMO networks," in *Proc. IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*. IEEE, 2022, pp. 1–6.

[12] D. Wang, M. Wu, Z. Wei, K. Yu, L. Min, and S. Mumtaz, "Uplink Secrecy Performance of RIS-based RF/FSO Three-Dimension Heterogeneous Networks," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2023.

[13] L. Wei, K. Wang, C. Pan, and M. Elkashlan, "Secrecy performance analysis of RIS-aided communication system with randomly flying eavesdroppers," *IEEE Wireless Communications Letters*, vol. 11, no. 10, pp. 2240–2244, 2022.

[14] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi, and L. Hanzo, "Ris-aided secure millimeter-wave communication under rf-chain impairments," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 952–963, 2024.

[15] A. Salem, K.-K. Wong, and C.-B. Chae, "Impact of phase-shift error on the secrecy performance of uplink RIS communication systems," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2023.

[16] W. Shi, J. Xu, W. Xu, C. Yuen, A. L. Swindlehurst, and C. Zhao, "On secrecy performance of RIS-assisted MISO systems over rician channels with spatially random eavesdroppers," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2024.

[17] J. Chen, Y.-C. Liang, H. V. Cheng, and W. Yu, "Channel estimation for reconfigurable intelligent surface aided multi-user mmwave MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 22, no. 10, pp. 6853–6869, 2023.

[18] K. Zhi, C. Pan, H. Ren, K. Wang, M. Elkashlan, M. Di Renzo, R. Schober, H. V. Poor, J. Wang, and L. Hanzo, "Two-timescale design for reconfigurable intelligent surface-aided massive mimo systems with imperfect csi," *IEEE Transactions on Information Theory*, vol. 69, no. 5, pp. 3001–3033, 2022.

[19] S. W. H. Shah, S. P. Deram, and J. Widmer, "On the effective capacity of RIS-enabled mmwave networks with outdated CSI," in *Proc. IEEE Conference on Computer Communications (IEEE INFOCOM)*. IEEE, 2023, pp. 1–10.

[20] K. Zhi, C. Pan, H. Ren, and K. Wang, "Power scaling law analysis and phase shift optimization of ris-aided massive mimo systems with statistical csi," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3558–3574, 2022.

[21] K. Zhi, C. Pan, G. Zhou, H. Ren, M. Elkashlan, and R. Schober, "Is ris-aided massive mimo promising with zf detectors and imperfect csi?" *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 10, pp. 3010–3026, 2022.

[22] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 375–388, 2020.

[23] Z. Zhang, J. Chen, Y. Liu, Q. Wu, B. He, and L. Yang, "On the secrecy design of star-ris assisted uplink noma networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 12, pp. 11 207–11 221, 2022.

[24] H. Jia, L. Ma, and S. Valaee, "Star-ris enabled downlink secure noma network under imperfect csi of eavesdroppers," *IEEE Communications Letters*, vol. 27, no. 3, pp. 802–806, 2023.

[25] S. Lin, Y. Xu, H. Wang, J. Gu, J. Liu, and G. Ding, "Secure multicast communications via ris against eavesdropping and jamming with imperfect csi," *IEEE Transactions on Vehicular Technology*, 2023.

[26] K. M. Hamza, S. Basharat, S. A. Hassan, and H. Jung, "On the Secrecy Performance of RIS-Enhanced Aerial Communication Under Imperfect CSI," in *Proc. IEEE IEEE International Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2023, pp. 1–6.

[27] S. Waqas Haider Shah, M. M. U. Rahman, A. N. Mian, A. Imran, S. Mumtaz, and O. A. Dobre, "On the impact of mode selection on effective capacity of device-to-device communication," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 945–948, 2019.

[28] S. W. H. Shah, M. M. U. Rahman, A. N. Mian, O. A. Dobre, and J. Crowcroft, "Effective capacity analysis of HARQ-enabled D2D communication in multi-tier cellular networks," *IEEE transactions on vehicular technology*, vol. 70, no. 9, pp. 9144–9159, 2021.

[29] G. Zhou, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "A framework of robust transmission design for irs-aided miso communications with imperfect cascaded channels," *IEEE Transactions on Signal Processing*, vol. 68, pp. 5092–5106, 2020.

[30] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in ris-aided miso system with hardware impairments," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1309–1313, 2021.

[31] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas part ii: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[32] K. Zhi, C. Pan, H. Ren, K. K. Chai, and M. Elkashlan, "Active ris versus passive ris: Which is superior with the same power budget?" *IEEE Communications Letters*, vol. 26, no. 5, pp. 1150–1154, 2022.

[33] C. Sun, C. She, C. Yang, T. Q. Quek, Y. Li, and B. Vucetic, "Optimizing resource allocation in the short blocklength regime for ultra-reliable and low-latency communications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 402–415, 2018.

[34] D. Qiao, M. C. Gursoy, and S. Velipasalar, "Secure wireless communication and optimal power control under statistical queueing constraints," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 628–639, 2011.

[35] J. Palacios, D. De Donno, and J. Widmer, "Lightweight and effective sector beam pattern synthesis with uniform linear antenna arrays," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 605–608, 2017.

[36] IEEE 802.11 working group, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications-Amendment 2: Enhanced Throughput for Operation in License-Exempt Bands Above 45 GHz," *IEEE Standard 802.11ay*, 2021.

[37] W. Tang, X. Chen, M. Z. Chen, J. Y. Dai, Y. Han, M. Di Renzo, S. Jin, Q. Cheng, and T. J. Cui, "Path loss modeling and measurements for reconfigurable intelligent surfaces in the millimeter-wave frequency band," *IEEE Transactions on Communications*, vol. 70, no. 9, pp. 6259–6276, 2022.

[38] Y. Zhang, J. Zhang, M. Di Renzo, H. Xiao, and B. Ai, "Reconfigurable intelligent surfaces with outdated channel state information: Centralized vs. distributed deployments," *IEEE Transactions on Communications*, vol. 70, no. 4, pp. 2742–2756, 2022.