On the Impact of Age of Channel Information on Secure RIS-assisted mmWave Networks

Syed Waqas Haider Shah*†, *Member, IEEE*, Marwa Qaraqe†, *Senior Member, IEEE*, Saud Althunibat‡, *Senior Member, IEEE*, and Joerg Widmer*, *Fellow, IEEE*
*IMDEA Networks Institute, Madrid, Spain
† College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar
‡Department of Computer Engineering, Faculty of Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan
{syed.waqas, joerg.widmer}@imdea.org, mqaraqe@hbku.edu.qa, saud.althunibat@qatar.tamu.edu

***Abstract*—Reconfigurable Intelligent Surfaces (RISs) have shown great prospects in securing mmWave communication from potential eavesdropping by configuring reflecting elements to strengthen the signal strength at the desired location and creating 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 studies the impact of the age of channel information on the secrecy performance of a RIS-assisted mmWave network. In particular, we investigate how outdated channel information affects the joint optimization of transmit beamforming and RIS configuration. 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capacity and demonstrate that adequate secrecy capacity can still be achieved even when channel information is slightly outdated, thus reducing the need for frequent RIS configuration.**

***Index Terms*—Secrecy capacity, RIS, mmWave networks, outdated channel estimates**

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 [1]. 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 utilizes reflecting surfaces to enhance the security of wireless communication by intelligently controlling the wireless propagation environment, making it a promising approach for future secure wireless networks. Initial studies on RIS-assisted PLS have delved into assessing the secrecy performance of wireless communication in different network settings [7–14]. While [7, 9] optimize RIS configurations to enhance the secrecy rates in a single-user scenario with one potential eavesdropper, they do not consider the impact of multiple users or eavesdroppers. The authors in [11] extend upon these works to a MIMO network in the presence of a multi-antenna eavesdropper, proposing meta-heuristic solutions for hybrid RIS configurations. Meanwhile, [10] provides secrecy outage probability of RIS-assisted SISO systems but lacks mechanisms for RIS configuration and to enhance the secrecy performance. Similarly, [12] explores secrecy performance in a RIS-assisted heterogeneous network by providing closed-form expression for the asymptotic secrecy outage probability. The aforementioned work have established valuable benchmarks for evaluating the secrecy performance of RIS-assisted wireless networks. Nevertheless, their reliance on perfect channel information for analysis raises concerns about the viability of the solutions provided therein.

In a practical RIS-assisted mmWave system, achieving perfect instantaneous channel state information (CSI) presents several complex challenges. First, 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 inter-

play 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 CSI, which results in large delays and higher complexity. Additionally, in a dynamic multi-user RIS-assisted mmWave network, CSI received by the BS may become outdated by the time they are received. In short, due to the rapid and unanticipated variations in a RIS-assisted mmWave channel, trying to maintain up-to-date CSI can be resource-intensive and complex. Therefore, it is important to assess the impact of the age of channel information on the secrecy performance of the network.

The authors in [15, 16] study the impact of imperfect channel estimates on secrecy performance. The authors in [15] provide a deep reinforcement learning-based solution to configure the RIS under imperfect channel estimates while the authors in [16] propose a secrecy rate maximization problem under the target secrecy rate constraint to optimize the number of RIS elements while also assuming imperfect CSI. Although these work study the impact of channel estimation errors in their model, they do not consider the age of channel information (outdatedness of CSI). The age of information is equally as important to investigate as it focuses on the temporal aspect of the channel estimates, emphasizing the potential decay of channel information over time.

To this end, this work advances the state-of-the-art by investigating the temporal impact of outdated CSI on the secrecy performance of a RIS-enabled mmWave network (RISE-MM) in the presence of multiple eavesdroppers. We propose joint optimization of transmit beamforming and RIS configuration, taking into account the influence of outdated CSI noise and interference from multiple users in the network. Specifically, we derive a closed-form expression for the cumulative noise effect due to outdated CSI and inter-user interference. Our simulation results highlight a strong relation between the age of channel information and the secrecy performance of a RIS-assisted mmWave network.

The remainder of the paper is structured as follows: Section II introduces the system model, while Section III delves into the channel modeling for the secure RIS-assisted mmWave network. In Section IV, we present the performance analysis, addressing the beamforming optimization problem at both the BS and the RIS. Section V then assesses the analytical findings through simulations, offering valuable insights. Finally, Section VI concludes the paper.

II. System Model

We consider a secure mmWave communication system with multiple users, as shown in Fig. 1, in which the users are divided into two groups based on the authentication process. The users authenticated by the BS are considered legitimate users of the network. Users who failed the authentication process but are still present in the network are grouped as unrecognized users, and they can potentially eavesdrop on the information shared by the BS to legitimate users [1]. Let $L\{l = (1, 2, ..., L)\}$ and $\Xi\{n = (1, 2, ..., \Xi)\}$ refer to legitimate users and eavesdroppers present in the network, respectively. In the proposed system model, we leverage a large RIS to increase (decrease) the received signal-to-interference-and-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 $\mathbf{H} \in \mathbb{C}^{N_R \times N_B}$, $\mathbf{h}^b_{l,u} \in \mathbb{C}^{1\times N_B}$, $\mathbf{h}^b_{n,e} \in \mathbb{C}^{1\times N_B}$, $\mathbf{g}_{l,u} \in \mathbb{C}^{1\times N_R}$, and $\mathbf{g}_{e,n} \in \mathbb{C}^{1\times N_R}$ be the channel coefficients of the channel between BS and RIS, BS and l^{th} legitimate user, BS and n^{th} potential eavesdropper, RIS and l^{th} legitimate user, and RIS and n^{th} potential eavesdropper, respectively. Since we are considering a RIS-assisted mmWave system model in which BS (RIS) performs beamforming towards RIS (l^{th} legitimate user), both $\mathbf{H}$ and $\mathbf{g}_{l,u}$ have dominant line-of-sight (LoS) path. Whereas, for rest of the channels, it is highly probable that a dominant LoS path may not exist. Therefore, we consider that $\mathbf{H}$ and $\mathbf{g}_{l,u}$ channels follow Rician fading, and $\mathbf{g}_{n,e}$, $\mathbf{h}^b_{l,u}$, and $\mathbf{h}^b_{n,e}$ follow Rayleigh fading.

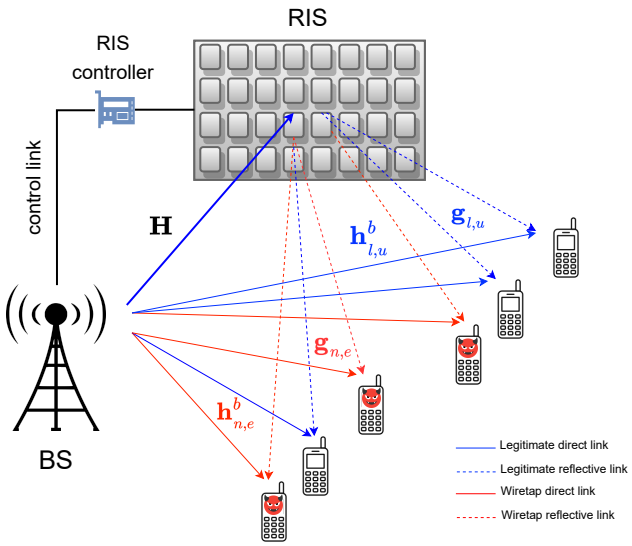

Fig. 1. RIS-enabled mmWave network (RISE-MM) with multiple legitimate users and potential eavesdroppers.

The BS sends a secret message to l^{th} legitimate user ($s_l \sim \mathcal{CN}(0, 1)$) through a RIS with a continuous linear transmit beamforming vector $\mathbf{v}_l$ ($\in \mathbb{C}^{N_B}$). Let $\mathbf{\Omega} \in \mathbb{C}^{N_R \times N_R}$

[1]To counter completely inactive or fully passive eavesdroppers, creating nulls throughout the network, except at the location of legitimate users using adaptive and narrow beamforming, could be the ideal scenario for a secure system. However, it requires perfect and up-to-date knowledge, not only of the communication channels but also of the entire environment, an optimal RIS configuration, and perfect beam training.

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. At l^{th} legitimate user, the received signal is composed of a desired signal (sum of direct and reflected signals) and inter-user interference caused by other legitimate users in the network, as shown in the following.

$$y_{l,u} = \underbrace{\{\mathbf{g}_{l,u}\mathbf{\Omega}\mathbf{H} + \mathbf{h}^b_{l,u}\}\mathbf{v}_l s_l}_{\text{desired signal}} + \underbrace{\textstyle\sum_{i=1,i\neq l}^{L}\{\mathbf{g}_{l,u}\mathbf{\Omega}\mathbf{H} + \mathbf{h}^b_{l,u}\}\mathbf{v}_i s_i}_{\text{Inter-user Interference}} + n_l, \tag{1}$$

where n_l is the complex additive White Gaussian noise (AWGN) with the following distribution $n_l \sim \mathcal{CN}(0, \sigma_l^2)$. The received signal at n^{th} potential eavesdropper is given by

$$y_{n,e} = \{\mathbf{g}_{\mathbf{e},\mathbf{n}}\mathbf{\Omega}\mathbf{H} + \mathbf{h}^b_{n,e}\}\sum_{l\in L}\mathbf{v}_l s_l + n_n \tag{2}$$

III. Channel Modelling with Outdated CSI

Perfect instantaneous channel estimates remain important for optimizing the system performance, it is almost impossible to acquire them at all times for practical RIS-assisted multi-user mmWave systems. In light of this, an intriguing idea comes into play in the form of leveraging outdated channel estimates, whereby the system intelligently makes use of CSI collected over a somewhat longer time period and manages to balance accuracy and overhead. With a more stable RIS configuration (also transmit beamforming) and less feedback signaling overhead, as well as an acceptable trade-off between system performance and real-time limitations, utilizing slightly outdated channel estimates seems to be a more practical and efficient approach. Let Δ_T denote the delay between the outdated CSI and the instantaneous CSI, then the relation between the outdated channel vector $\alpha(t)$ and the instantaneous channel vector $\alpha(t+\Delta_T)$ becomes

$$\alpha(t+\Delta_T) = \rho\alpha(t) + \sqrt{1-\rho^2}\hat{\alpha}(t+\Delta_T). \tag{3}$$

Where $\hat{\alpha}(t+\Delta_T)$ is the estimated version of $\alpha(t+\Delta_T)$, ρ $(0 \leq \rho \leq 1)$ is a coefficient that defines the correlation strength based on the age of channel information [2]. The channel uncertainty model enables us to determine the signal received at l^{th} legitimate user when system operates under the influence of outdated channel estimates [3].

[2]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: $\rho = J_0(2\pi f^D\Delta_T)$. $\rho = 0$ indicates no CSI is available from the previous time slot, and $\rho = 1$ implies the effect of outdated CSI is eliminated.

[3]System operation refers to packet scheduling and transmit beamforming optimization at BS and phase configuration of reflecting elements at RIS [17].

Thus, (1) under channel uncertainty model given in (3) becomes

$$y^{\text{out}}_{l,u} = \underbrace{\big[\rho_l\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H} + \rho_{o,u}\hat{\mathbf{h}}^b_{l,u}\big]\mathbf{v}_l s_l}_{\text{desired signal}} + \underbrace{\big[\bar{\rho}_l\mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H} + \bar{\rho}_{o,u}\mathbf{w}^d_{l,u}\big]\mathbf{v}_l s_l}_{\text{outdated CSI noise}} + \underbrace{\sum_{i=1,i\neq l}^{L}\big[\rho_l\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H} + \rho_{o,u}\hat{\mathbf{h}}^b_{l,u}\big]\mathbf{v}_i s_i + \sum_{i=1,i\neq l}^{L}\underbrace{\{\bar{\rho}_l\mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H} + \bar{\rho}_{o,u}\mathbf{w}^d_{l,u}\}\mathbf{v}_i s_i}_{\text{outdated CSI noise}}}_{\text{inter-user interference}} + n_l, \tag{4}$$

where $\hat{\mathbf{g}}_{l,u} = \mathbf{g}_{l,u}(t)$, $\hat{\mathbf{h}}^b_{l,u} = \mathbf{h}^b_{u,l}(t)$, $\mathbf{w}^R_{l,u} = \hat{\mathbf{g}}_{l,u}(t+\Delta_T)$, and $\mathbf{w}^d_{l,u} = \hat{\mathbf{h}}^b_{u,l}(t+\Delta_T)$. Since, the channels (RIS to l^{th} user and BS to l^{th}) change independently, the correlation strength between instantaneous and outdated estimates of the respective channels behave differently. Therefore, we introduce ρ_l and $\rho_{o,u}$ as the correlation strength for the channel between RIS and l^{th} user and BS and l^{th} user, respectively. Moreover, $\bar{\rho}_l = \sqrt{1-\rho_l^2}$ and $\bar{\rho}_{o,u} = \sqrt{1-\rho_{o,u}^2}$. Similarly, the received signal at n^{th} potential eavesdropper under the influence of channel uncertainty model can be calculated using the following expression.

$$y^{\text{out}}_{n,e} = \underbrace{\big[\rho_e\hat{\mathbf{g}}_{n,e}\mathbf{\Omega}\mathbf{H} + \rho_{o,e}\hat{\mathbf{h}}^b_{n,e}\big]\sum_{l\in L}\mathbf{v}_l s_l}_{\text{expected signal copy at n}^{\text{th}}\text{ eve}} + \underbrace{\big[\bar{\rho}_e\hat{\mathbf{w}}^R_{n,e}\mathbf{\Omega}\mathbf{H} + \bar{\rho}_{o,e}\hat{\mathbf{w}}^d_{n,e}\big]\sum_{l\in L}\mathbf{v}_l s_l}_{\text{outdated CSI noise at n}^{\text{th}}\text{ eve}} + n_n, \tag{5}$$

where, ρ_e $(\rho_{o,u})$ is the correlation strength between the outdated and instantaneous estimates of the channel between RIS and n^{th} eavesdropper (BS and n^{th} eavesdropper), and $\bar{\rho}_e = \sqrt{1-\rho_e^2}$ and $\bar{\rho}_{o,e} = \sqrt{1-\rho_{o,e}^2}$.

Since we know the received signal at l^{th} legitimate user and n^{th} eavesdropper from (4) and (5), respectively, we now aim to find the Shannon capacity of the respective channels. Let $C^{\text{out}}_{l,u}\{= \log_2(1+\Gamma^{\text{out}}_{l,u})\}$ and $C^{\text{out}}_{n,e}\{= \log_2(1+\Gamma^{\text{out}}_{n,e})\}$ be the achievable capacity given the outdated channel estimates at l^{th} user and n^{th} eavesdropper, respectively, and $\Gamma^{\text{out}}_{l,u}$ and $\Gamma^{\text{out}}_{n,e}$ are the received SINR of the respective channels. The received SINR given the channel uncertainty model becomes

$$\Gamma^{\text{out}}_{l,u} = \frac{\mathbf{X}^{(1)}_{l,u}\mathbf{v}_l^2}{\sum_{i=1,i\neq l}^{L}\mathbf{v}_i^2\mathbf{X}^{(1)}_{l,u} + \sum_{i=1}^{L}\mathbf{v}_i^2\mathbf{X}^{(2)}_{l,u} + \sigma_l^2}, \qquad \Gamma^{\text{out}}_{n,e} = \frac{\mathbf{X}^{(1)}_{n,e}\mathbf{v}_l^2}{\sum_{i\in L,i\neq l}\mathbf{v}_i^2\mathbf{X}^{(1)}_{n,e} + \sum_{i\in L}\mathbf{v}_i^2\mathbf{X}^{(2)}_{n,e} + \sigma_n^2}, \tag{6}$$

where $\mathbf{X}^{(1)}_{l,u} = \big|\rho_l\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H} + \rho_{o,u}\hat{\mathbf{h}}^b_{l,u}\big|^2$, $\mathbf{X}^{(2)}_{l,u} = \big|\bar{\rho}_l\mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H} + \bar{\rho}_{o,u}\mathbf{w}^d_{l,u}\big|^2$, $\mathbf{X}^{(1)}_{n,e} = \big|\rho_e\hat{\mathbf{g}}_{n,e}\mathbf{\Omega}\mathbf{H} + \rho_{o,e}\hat{\mathbf{h}}^b_{n,e}\big|^2$, and $\mathbf{X}^{(2)}_{n,e} = \big|\bar{\rho}_e\hat{\mathbf{w}}^R_{n,e}\mathbf{\Omega}\mathbf{H} + \bar{\rho}_{o,e}\hat{\mathbf{w}}^d_{n,e}\big|^2$. The variance of complex AWGN noise of the respective channels are given by σ_l^2 and σ_n^2. Our goal is to find the optimal secrecy capacity of the proposed multi-user RIS-assisted mmWave system model with outdated channel estimates. To this end, the next section first calculates the secrecy capacity of the legitimate user and then presents a mechanism to maximize it.

IV. Performance Analysis of Secure RISE-MM

The secrecy capacity is a key performance metric when developing a secure communication system. 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. 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 in the following

$$C_{s,l}^{\text{out}} = [C_{l,u}^{\text{out}} - C_{n,e}^{\text{out}}]^{+}. \tag{7}$$

Where $[C_{l,u}^{\text{out}} - C_{n,e}^{\text{out}}]^{+} = \max\{0, [C_{l,u}^{\text{out}} - C_{n,e}^{\text{out}}]\}$. The maximization of $C_{s,l}$ is to be achieved through joint optimization of transmit beamforming vector and phase shift matrix at BS and RIS, respectively. The optimization problem at hand becomes

$$\begin{aligned}
(\text{P1}) \quad & \max_{\mathbf{v}_l, \mathbf{\Omega}} \quad \log_2\left(\frac{1+\frac{\mathbf{X}_{l,u}^{(1)}\mathbf{v}_l^2}{\sum_{i=1,i\neq l}^{L}\mathbf{v}_i^2\mathbf{X}_{l,u}^{(1)}+\sum_{i=1}^{L}\mathbf{v}_i^2\mathbf{X}_{l,u}^{(2)}+\sigma_l^2}}{1+\frac{\mathbf{X}_{n,e}^{(1)}\mathbf{v}_l^2}{\sum_{i\in L,i\neq l}\mathbf{v}_i^2\mathbf{X}_{n,e}^{(1)}+\sum_{i\in L}\mathbf{v}_i^2\mathbf{X}_{n,e}^{(2)}+\sigma_n^2}}\right) \\
\text{s.t.} \quad & (c1) \quad \|\mathbf{v}_l\|^2 \leq P_{\text{BS}} \\
& (c2) \quad |\alpha_r e^{j\theta_r}| = 1, 0 < \theta_r < 2\pi, \forall_r \in N_R
\end{aligned} \tag{8}$$

where P_{BS} is the transmit power of the BS. 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 1) and the reflection coefficient matrix at RIS (constraint 2). Moreover, the unit modulus constraint imposed on each reflecting cell at the RIS is non-convex. Furthermore, we note that constraints (c1) and (c2) are independent of each other, encompassing variables $\mathbf{v}_l$ 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, we aim to maximize problem given in (P1) by optimizing the transmit beamforming vector ($\mathbf{v}_l$) while fixing the reflection coefficient of the RIS elements (fixed $\mathbf{\Omega}$). Let $\sigma_{l,u}^2$ and $\sigma_{n,e}^2$ is the cumulative noise effect (sum of the effects of outdated CSI noise and inter-user interference) at l^{th} legitimate user and n^{th} eavesdropper, respectively. Then, these can be calculated using: $\sigma_{l,u}^2 = \sum_{i=1,i\neq l}^{L}\mathbf{v}_i^2\mathbf{X}_{l,u}^{(1)} + \sum_{i=1}^{L}\mathbf{v}_i^2\mathbf{X}_{l,u}^{(2)}$ and $\sigma_{n,e}^2 = \sum_{i\in L,i\neq l}\mathbf{v}_i^2\mathbf{X}_{n,e}^{(1)} + \sum_{i\in L}\mathbf{v}_i^2\mathbf{X}_{n,e}^{(2)}$. Therefore, (P1) in terms of cumulative noise can be reformulated as follows.

$$\begin{aligned}
(\text{P1a}) \quad & \max_{\mathbf{v}_l} \quad \log_2\left(\frac{1+1/(\sigma_{l,u}^2+\sigma_l^2)\mathbf{X}_{l,u}^{(1)}\mathbf{v}_l^2}{1+1/(\sigma_{n,e}^2+\sigma_n^2)\mathbf{X}_{n,e}^{(1)}\mathbf{v}_l^2}\right) \\
& \text{s.t.} \quad \|\mathbf{v}_l\|^2 \leq P_{\text{BS}}
\end{aligned} \tag{9}$$

We can eliminate $\log_2$ from (P1a) due to its strictly monotonically increasing nature, and $\mathbf{v}_l^2 = \mathbf{v}_l^H\mathbf{v}_l$ where $\mathbf{v}_l^H$ is the conjugate transpose of $\mathbf{v}_l$. Thus, (P1a) can be further reformulated as

$$\begin{aligned}
(\text{P1b}) \quad & \max_{\mathbf{v}_l} \quad \frac{1+1/(\sigma_{l,u}^2+\sigma_l^2)\mathbf{v}_l^H\mathbf{X}_{l,u}^{(1)}\mathbf{v}_l}{1+1/(\sigma_{n,e}^2+\sigma_n^2)\mathbf{v}_l^H\mathbf{X}_{n,e}^{(1)}\mathbf{v}_l} \\
& \text{s.t.} \quad \|\mathbf{v}_l\|^2 \leq P_{\text{BS}}
\end{aligned} \tag{10}$$

In (P1b), we note that the transmit beamforming vector $\mathbf{v}_l$ at BS is independent of the variables $\mathbf{X}_{l,u}^{(1)}$, $\mathbf{X}_{n,e}^{(1)}$, and cumulative and thermal noise at l^{th} legitimate user and n^{th} eavesdropper; thus, these become constants with respect to $\mathbf{v}_l$. To this end, the optimal solution to (P1b) comes out to be [18].

$$\mathbf{v}_l^{\text{opt}} = \sqrt{P_{\text{BS}}}\lambda_{max}\left\{\left(\frac{\mathbf{X}_{n,e}^{(1)}}{\sigma_{n,e}^2+\sigma_n^2}+\frac{I_{N_B}}{P_{\text{BS}}}\right)^{-1}\left(\frac{\mathbf{X}_{l,u}^{(1)}}{\sigma_{l,u}^2+\sigma_l^2}+\frac{I_{N_B}}{P_{\text{BS}}}\right)\right\}, \tag{11}$$

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 here that the optimal transmit beamforming vector in (11) is subject to the outdated channel estimates. Therefore, it is essential to determine the impact of outdated channel estimates and inter-user interference (at both l^{th} legitimate user and n^{th} eavesdropper) on $\mathbf{v}_l^{\text{opt}}$. For this purpose, Lemma 1 produces the closed-form expression of the cumulative effect of outdated CSI and inter-user interference at l^{th} legitimate user.

Lemma 1. *The cumulative effect of outdated CSI and inter-user interference on the optimal transmit beamforming vector ($\mathbf{v}_l^{opt}$) can be calculated using the following expression.*

$$\begin{aligned}
\sigma_{l,u}^2 = & \sum_{i=1,i\neq l}^{L}\sum_{b=1}^{N_B}|v_{i,b}|^2\left[\rho_l^2(1-\alpha_{l,u}^{(R)2}) + \bar{\rho}_l^2(1-\beta_{l,u}^{(R)2})v_{l,b}\right] \\
& + \sum_{i=1,i\neq l}^{L}\mathbf{v}_i^2\left[\rho_{o,u}^2(1-\alpha_{l,u}^{(d)2}) + \bar{\rho}_{o,u}^2(1-\beta_{l,u}^{(d)2})\mathbf{v}_l\right].
\end{aligned} \tag{12}$$

where $\alpha_{l,u}^{(R)2}$ and $\beta_{l,u}^{(R)2}$ indicates mean of Rician variable $|g_{l,u}(t)|$ and $|\hat{g}_{l,u}(t+\Delta_T)|$, respectively, and $\alpha_{l,u}^{(d)2}$ and $\beta_{l,u}^{(d)2}$ indicates mean of Rayleigh variable $|h_{l,u}^b(t)|$ and $|\hat{h}_{l,u}^b(t+\Delta_T)|$, respectively.

Proof: Given in Appendix A

One can also find the impact of outdated CSI and interference at n^{th} eavesdropper, for which the detail is similar to that in Lemma 1 and therefore omitted here due to space constraints. The solution in (11) incorporates the effects of noise generated by the fact that the CSI is outdated; thus, it provides us the optimal transmit beamforming vector given the channel estimates available at the BS are outdated. Next, we aim to find the optimal RIS configuration by solving the optimization problem given in (P1) for the constraint imposed by the RIS elements (second constraint).

B. Beamforming Optimization at the RIS

Given the optimal transmit beamforming vector, we aim to find the phase shifts of the RIS reflecting elements which maximizes the received SINR at l^{th} legitimate user while

$$\text{(P2a)} \quad \max_{\mathbf{\Omega}} \quad \log_2\left(\frac{1+1/(\sigma_{l,u}^2+\sigma_l^2)\left|\sum_{b=1}^{N_B}\sum_{r=1}^{N_R}\rho_l\hat{g}_{r,l}\alpha_r h_{b,r}e^{j(\theta_{r,l}+\theta_r+\theta_{b,r})}v_{l,b}^{\text{opt}}+\sum_{b=1}^{N_B}\rho_{o,u}\hat{h}_{b,l}e^{j\theta_{b,l}}v_{l,b}^{\text{opt}}\right|^2}{1+1/(\sigma_{n,e}^2+\sigma_n^2)\left|\sum_{b=1}^{N_B}\sum_{r=1}^{N_R}\rho_e\hat{g}_{r,n}\alpha_r h_{b,r}e^{j(\theta_{r,n}+\theta_r+\theta_{b,r})}v_{l,b}^{\text{opt}}+\sum_{b=1}^{N_B}\rho_{o,e}\hat{h}_{b,n}e^{j\theta_{b,n}}v_{l,b}^{\text{opt}}\right|^2}\right) \tag{14}$$
$$\text{s.t.} \quad |\alpha_r e^{j\theta_r}| = 1, 0 < \theta_r < 2\pi, \forall_r \in N_R$$

simultaneously minimizing the received SINR at n^{th} eavesdropper. To this end, the problem (P1) becomes

$$\text{(P2)} \max_{\mathbf{\Omega}} \log_2\left(\frac{1+1/(\sigma_{l,u}^2+\sigma_l^2)\left|\rho_l\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H}+\rho_{o,u}\hat{\mathbf{h}}_{l,u}^b\right|^2\mathbf{v}_l^{2(\text{opt})}}{1+1/(\sigma_{n,e}^2+\sigma_n^2)\left|\rho_e\hat{\mathbf{g}}_{n,e}\mathbf{\Omega}\mathbf{H}+\rho_{o,e}\hat{\mathbf{h}}_{n,e}^b\right|^2\mathbf{v}_l^{2(\text{opt})}}\right)$$
$$\text{s.t.} \quad |\alpha_r e^{j\theta_r}| = 1, 0 < \theta_r < 2\pi, \forall_r \in N_R \tag{13}$$

By representing the respective channels in their polar form, as shown in Fig. 2, and after some simplification steps, (13) can be reformulated as given in (14), shown at the top of the page. In (14), $\hat{g}_{r,l}$ $(\theta_{r,l})$, α_r (θ_r), $h_{r,l}$ $(\theta_{b,r})$, $\hat{h}_{b,l}$ $(\theta_{b,l})$, $\hat{g}_{r,n}$ $(\theta_{r,n})$, and $\hat{h}_{b,n}$ $(\theta_{b,n})$ are the envelope (phase) of the respective channels.

The maximization problem in (14) 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 l^{th} legitimate user with the phase of the outdated RIS-assisted channel between the BS and the l^{th} legitimate user. Concurrently, the outdated direct channel between the BS and the n^{th} eavesdropper should be out of phase with the outdated RIS-assisted channel between the BS and the n^{th} 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 l^{th} legitimate user (n^{th} eavesdropper) can be calculated

$$\theta_r^* = \arg\max_{0<\theta_r<2\pi} \frac{\gamma_{l,u}^{\text{out}}}{(\sigma_{l,u}^2+\sigma_l^2)} = \left\{\theta_{b,l}-(\theta_{r,l}+\theta_{b,r})\right\}$$
$$\theta_r^* = \arg\min_{0<\theta_r<2\pi} \frac{\gamma_{n,e}^{\text{out}}}{(\sigma_{n,e}^2+\sigma_n^2)} = \left\{\theta_{b,n}-(\theta_{r,n}+\theta_{b,r})\right\}, \tag{15}$$

where $\gamma_{l,u}^{\text{out}} = \left|\sum_{b=1}^{N_B} v_{l,b}^{\text{opt}}(\sum_{r=1}^{N_R}\rho_l\hat{g}_{r,l}\alpha_r h_{b,r}+\rho_{o,u}\hat{h}_{b,l})\right|^2$ and $\gamma_{n,e}^{\text{out}} = \left|\sum_{b=1}^{N_B} v_{l,b}^{\text{opt}}(\sum_{r=1}^{N_R}\rho_e\hat{g}_{r,n}\alpha_r h_{b,r}+\rho_{o,e}\hat{h}_{b,n})\right|^2$. The phase shift in (15) maximizes (minimizes) the received SINR at l^{th} legitimate user (n^{th} eavesdropper) under the influence of the 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 (15) 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.

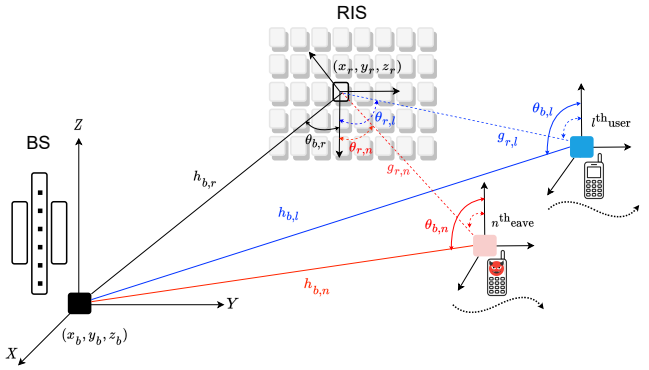

Fig. 2. Polar representation of the direct and RIS-assisted legitimate and wiretap links to l^{th} user and n^{th} eavesdropper, respectively.

V. Evaluation and Discussion

In this section, we evaluate the analytical findings using Monte Carlo simulations. In particular, we aim to investigate the impact of the age of channel information on the secrecy performance of a RIS-assisted mmWave network and find a pragmatic tradeoff between RIS configuration frequency and the secrecy performance of the network. We consider a uniform linear array at BS with a size of $N_B = 32$ and a rectangular array at RIS with dimensions $N_R = 64\times64$ (unless otherwise specified). The antenna (reflecting) element spacing at BS (RIS) is $\lambda/2$. All the channels follow Rayleigh fading (BS → RIS → legitimate user follows Rician fading due to the presence of a strong LoS component) and are modeled using

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

the IEEE 802.11ay multipath fading channel model, employing a quasi-deterministic approach. Additionally, our system employs the IEEE 802.11ay standard and utilizes a codebook of beam patterns for beam training at the RIS. Furthermore, we adopt the design approach described in [19] to generate beam patterns with varying beam widths. Other system parameters are set as follows: $f_c = 28GHz$, $n_l = -60dBm$.

Fig. 3 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. 3(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. 3(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. 3(b), where the channel correlation strength decreases exponentially fast with higher user mobility in the near-field of the RIS. This investigation provides valuable insights into how a RIS-assisted mmWave channel ages over time and underscores the factors that directly influence the channel aging process. Further, this knowledge is leveraged for optimizing beamforming at both the BS and the RIS.

Fig. 4 presents an investigation into the impact of the age of channel information on secrecy capacity. In this context, Fig. 4(a) shows that a strong correlation between outdated and instantaneous 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 ($0.4 < \rho < 0.8$). This demonstrates that infrequent RIS configuration, even with outdated CSI, can still deliver satisfactory system performance. This, in turn, reduces the high signaling overhead and complexity associated with frequent channel estimation and RIS configuration. Additionally, it demonstrates that the proposed beamforming design performs better with a larger RIS, ultimately achieving higher secrecy capacity. Fig. 4 (b) reveals an increase in secrecy capacity with an increase in the BS transmit power. However, this growth is bounded by the age of channel information. This particular insight holds significant importance for system design since increasing transmit power may not necessarily yield improved secrecy capacity when the estimated and actual channel states exhibit only loose correlations. This is primarily because, with weak channel correlation strength, the configuration of the RIS becomes suboptimal. As a result, the reflected beam may point to an area where the legitimate user is no longer located due to the user's mobility. Therefore, in such a scenario, an increase in BS transmit power does not translate into a corresponding increase in secrecy capacity.

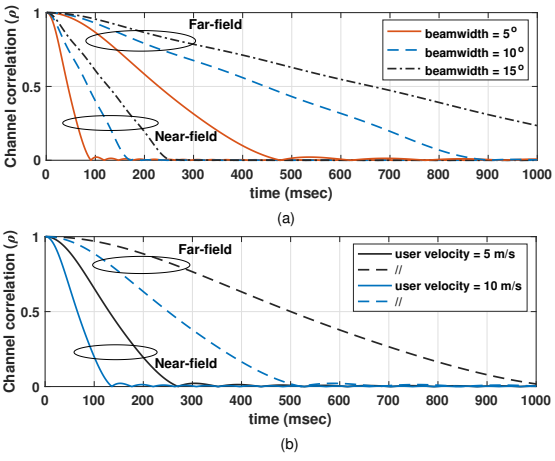

Fig. 3. Age of channel information of a RIS-assisted mmWave link over time with user mobility in near-field and far-field of the RIS; (a) for different beam widths, (b) for different user velocity.

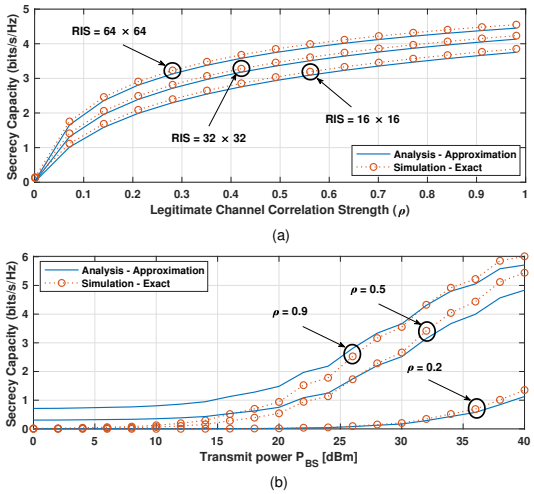

Fig. 4. Impact of channel correlation strength on secrecy performance; secrecy capacity vs (a) legitimate channel correlation strength for different RIS size, (b) transmit power of the BS.

VI. Conclusion

This work has investigated the influence of outdated channel information on the joint optimization of transmit beamforming and RIS configuration, aiming to enhance the secrecy performance of a RIS-assisted mmWave network. We have derived a closed-form expression for the cumulative noise effect resulting from outdated channel information and inter-user interference and have examined its impact on the received SINR at both the legitimate user and potential eavesdropping locations. Our Monte-Carlo simulations have revealed that the proposed system can achieve sufficient secrecy capacity

even when outdated channel information is used for RIS configuration. It has enabled us to tune system parameters that ensure enhanced secrecy performance while minimizing the complexity and costs associated with channel estimation and frequent RIS configuration.

ACKNOWLEDGMENT

This research work was sponsored by NATO Science for Peace and Security Programme under grant SPS G5797 and the Spanish Ministry of Economic Affairs and Digital Transformation under European Union NextGeneration-EU projects TSI-063000-2021-59 RISC-6G. Syed Waqas Haider Shah work was supported by MSCA-PF project RISE-MM (101061011) funded by the European Union Horizon Europe program.

APPENDIX A
PROOF OF LEMMA 1

The cumulative noise effect at l^{th} legitimate user is

$$\sigma^2_{l,u} = \mathbb{E}\Big[\textstyle\sum_{i=1,i\neq l}^{L} \mathbf{v}_i^2 \big|\rho_l \hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H} + \rho_{o,u}\hat{\mathbf{h}}^b_{l,u}\big|^2\Big] + \mathbb{E}\Big[\textstyle\sum_{i=1}^{L} \mathbf{v}_i^2 \big|\bar{\rho}_l \mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H} + \bar{\rho}_{o,u}\mathbf{w}^d_{l,u}\big|^2\Big]. \tag{16}$$

By separating the direct and RIS-assisted channels,

$$\begin{aligned}\sigma^2_{l,u} = &\sum_{i=1,i\neq l}^{L} \rho_l^2 \mathbb{E}\big[\big|\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H}\mathbf{v}_i\big|^2\big] + \sum_{i=1,i\neq l}^{L} \rho_{o,u}^2 \mathbf{v}_i^2 \mathbb{E}\big[|\hat{\mathbf{h}}^b_{l,u}|^2\big] \\ &+ \sum_{i=1}^{L} \bar{\rho}_l^2 \mathbb{E}\big[\big|\mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H}\mathbf{v}_i\big|^2\big] + \sum_{i=1}^{L} \bar{\rho}_{o,u}^2 \mathbf{v}_i^2 \mathbb{E}\big[|\mathbf{w}^d_{l,u}|^2\big].\end{aligned} \tag{17}$$

From here, we can see that: $\mathbb{E}\big[|\hat{\mathbf{h}}^b_{l,u}|^2\big] = \sigma^2_{\hat{h}^b_{l,u}} = 1 - \alpha^{2(d)}_{l,u}$ and $\mathbb{E}\big[|\hat{\mathbf{w}}^b_{u,l}|^2\big] = \sigma^2_{\hat{w}^b_{l,u}} = 1 - \beta^{2(d)}_{l,u}$. Where $\alpha^{2(d)}_{l,u}$ and $\beta^{2(d)}_{l,u}$ are the average value of channel estimates at time t and $t+\Delta_T$, respectively. On the other hand, to find $\mathbb{E}\big[\big|\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H}\mathbf{v}_i\big|^2\big]$ and $\mathbb{E}\big[\big|\mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H}\mathbf{v}_i\big|^2\big]$, we apply standard ensemble average method for matrices to find the closed-form expression, for which the detail is similar to that in Lemma 1 of [20] and therefore omitted here for brevity. After some simplification steps, the final expressions come out to be the following: $\mathbb{E}\big[\big|\hat{\mathbf{g}}_{l,u}\mathbf{\Omega}\mathbf{H}\mathbf{v}_i\big|^2\big] = \rho_l^2(1-\alpha^{2(R)}_{l,u})\sum_{b=1}^{N_B}|v_{i,b}|^2$ and $\mathbb{E}\big[\big|\mathbf{w}^R_{l,u}\mathbf{\Omega}\mathbf{H}\mathbf{v}_i\big|^2\big] = \bar{\rho}_l^2(1-\beta^{2(R)}_{l,u})\sum_{b=1}^{N_B}|v_{i,b}|^2$. Finally, by substituting these results in (17), and after some simplification steps, the final expression for cumulative noise effect at l^{th} legitimate user comes out to be the one given in (12).

REFERENCES

[1] 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.

[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 and Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[3] S. Waqas Haider 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," 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, 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 VTC 2023-Spring*.

[7] F. Keming, L. Xiao, H. Yu, J. Shi, and C. Yijian, "Physical layer security enhancement exploiting intelligent reflecting surface," *IEEE Communications Letters*, vol. 25, no. 3, 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, 2020.

[9] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, 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, 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 VTC 2022-Spring*, 2022.

[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*, 2023.

[13] L. Wei, Wang, C. Pan, and M. E, "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] H. Lei, F. Yang, I. S. Ansari, H. Liu, K. J. Kim, and T. A. Tsiftsis, "Secrecy Outage Performance Analysis for Uplink CR-NOMA Systems With Hybrid SIC," *IEEE Internet of Things Journal*, vol. 10, no. 15, 2023.

[15] H. Yang, Z. Xiong, J. Zhao, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Transactions on Wireless Communications*, vol. 20, 2020.

[16] 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 INFOCOM WKSHPS*, 2023, pp. 1–6.

[17] S. Waqas Haider Shah, R. Li, M. Mahboob Ur Rahman, A. Noor Mian, W. Aman, and J. Crowcroft, "Statistical QoS guarantees of a device-to-device link assisted by a full-duplex relay," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, p. e4339, 2021.

[18] 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.

[19] 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, 2016.

[20] S. Waqas Haider Shah, S. Pavan Deram, and J. Widmer, "On the Effective Capacity of RIS-enabled mmWave Networks with Outdated CSI," in *Proc. IEEE International Conference on Computer Communications (IEEE INFOCOM)*, 2023, pp. 1–10.