On the Secrecy-Reliability Performance Trade-off for NOMA-enabled 5G mmWave Networks

Sourabh Solanki*, Devendra S. Gurjar‡, Pankaj K. Sharma†, Shree K. Sharma*, and Symeon Chatzinotas*

*Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
†Department of ECE, National Institute of Technology Silchar, India
‡Department of ECE, National Institute of Technology Rourkela, India

Email: {sourabh.solanki,shree.sharma,symeon.chatzinotas}@uni.lu, devendra.gurjar@ieee.org, sharmap@nitrkl.ac.in

Abstract—The evolution of 5G wireless networks poses significant research challenges such as securing the user data, maintaining certain latency and reliability requirements etc. However, it can be challenging to simultaneously meet these performance requisites, which may lead to resort to a trade-off among different metrics. This paper investigates the secrecy-reliability performance trade-off (SRPT) for non-orthogonal multiple access (NOMA)-based millimeter wave (mmWave) networks. Herein, we consider two end-users, namely primary and secondary, which are served by an mmWave base station using downlink NOMA. Besides, a passive eavesdropper lying in the vicinity of these end-users attempts to intercept their legitimate message signals. For this set-up, we derive the closed-form expressions of the outage probability (OP) of a targeted end-user and intercept probability (IP) of the eavesdropper to analyze the SRPT of the system. We further propose a low-complexity average channel state information (CSI)-based power allocation strategy to improve the reliability of a targeted user while maintaining its information secrecy. Moreover, we obtain the condition under which NOMA guarantees superior secrecy performance than that of orthogonal multiple access (OMA) scheme. We corroborate our theoretical analysis via simulation results presented in terms of IP and OP.

Index Terms—Millimeter wave, non-orthogonal multiple access (NOMA), physical layer security, performance analysis.

I. INTRODUCTION

MILLIMETER-wave (mmWave) communications have recently received tremendous research interests due to the availability of large bandwidth resources to satiate the capacity demands of ultra-dense beyond fifth-generation (B5G) wireless networks [1]. However, despite ample spectrum resources at very high frequencies, mmWave communications face challenges to support massive connectivity for users. Since the mmWave transmissions are highly directional, the channels pertaining to end-users can be highly correlated [2]. More importantly, this correlation is favourable for non-orthogonal multiple access (NOMA)-based communications [3]. Hence, the integration of NOMA to mmWave communications is quite appealing to reap the benefits of very large bandwidth while providing connectivity simultaneously to a large number of devices in ultra-dense wireless networks. In literature, various research works have directed their attention towards NOMA-based mmWave networks [4]-[7]. Specifically, in [4], the authors have analyzed the capacity of NOMA-based mmWave massive MIMO systems. While the authors in [5] have considered a NOMA scheme to exploit finite resolution analog beamforming in mmWave networks, the work in [6] investigated the spectrum- and energy-efficient schemes for NOMA-based mmWave MIMO systems. The authors in [7] have recently carried-out the coverage analysis of cooperative NOMA-based mmWave networks.

On another front, owing to the proliferating data demands and growing reliance on sensitive information (e.g., financial data, medical records) transmission over the wireless medium, B5G networks are more vulnerable to security breaches. Consequently, physical layer security (PLS) has gained significant importance recently due to its capability of restraining the eavesdropping attacks while complementing the traditional cryptography methods [8], [9]. In recent years, a few works have studied the PLS separately for the NOMA-based [10], [11] and mmWave networks [12]. An initial attempt of considering PLS for NOMA-mmWave networks has been made in [13] and further some design aspects of these systems have been investigated in [14]-[16]. For instance, in [14], the authors have examined PLS for NOMA-mmWave networks with instantaneous channel state information (CSI)-enabled power allocation strategy to satisfy the quality of service (QoS) of a targeted user. Further, authors in [15] have addressed energy efficiency problem whereas stochastic geometry framework has been adopted in [16] to investigate the performance of NOMA-mmWave networks.

The evolving mmWave-based 5G wireless networks demand various QoS requirements, e.g., data privacy, low latency, and high reliability [17], [18]. Nonetheless, it can be challenging to simultaneously meet these performance requisites, which may lead to resort to a trade-off among different metrics. In light of the above, we are motivated to investigate the secrecy-reliability performance trade-off (SRPT) for a NOMA-based mmWave network which is an open problem. We focus on two downlink NOMA end-users (i.e., primary and secondary) served by an mmWave base station in the presence of a passive eavesdropper trying to intercept their legitimate message signals. We derive the closed-form expressions of the outage probability (OP) of a targeted end-user and intercept probability (IP) of the eavesdropper to analyze the SRPT of the system. Here, alongside various competitive NOMA power allocation strategies, we especially develop a low-complexity
average CSI-assisted end-user performance-based power allocation strategy to satisfy certain QoS (a.k.a. reliability) of a targeted user while maintaining the information secrecy. We obtain the condition under which NOMA guarantees superior secrecy performance than that of orthogonal multiple access (OMA) scheme. Finally, we present useful insights based on our SRPT analysis for the considered system.

II. System Model

As shown in Fig. 1, we consider a NOMA-enabled [10] two end-users downlink mmWave wireless network where a base station (BS) simultaneously serves the two end-users, namely primary user (PU) and secondary user (SU). The PU is referred so as it is a priority user located at the cell-edge whose reliability is to be guaranteed. Note that a two-user NOMA scheme is adopted in the 3GPP LTE-A standard [19], [20]. A coexisting passive eavesdropper (Eve) attempts to opportunistically intercept the secret information intended for either PU or SU by aligning itself towards the main beam. Hereby, we consider that the PU and SU are in the line-of-sight (LOS) to the BS. At mmWave frequencies, the LOS path is usually very strong compared with the non-LOS (NLOS) paths. In general, NLOS paths experience more than 20 dB loss compared with the LOS [7]. Further, a link of distance $d$ can be considered as LOS with probability $e^{-c d}$, where $c = \mu E[Z]/\pi$ represents a blockage parameter with $\mu$ and $E[Z]$ as the blockage density and average perimeter of blockage objects, respectively [7], [21]. We assume the directional beamforming at each of the transmitting and receiving nodes. For this purpose, a sectored antenna model$^1$ is adopted having directional antenna gain $G_i(\theta)$ with $i \in \{b, p, s, e\}$ expressed as [22]

$$G_i(\theta) = \begin{cases} G_{i,m}, & |\theta| \leq \frac{\phi}{2}, \\ G_{i,s}, & \text{otherwise}, \end{cases}$$

where $G_{i,m}$ is the main lobe gain, $G_{i,s}$ is the side/back lobe gain, $\phi$ is the antenna beamwidth, and $\theta$ is the angle off the boresight direction. Let the channels of links from BS to PU, SU, and Eve are denoted as $h_p$, $h_s$, and $h_e$, respectively which follow independent Nakagami-$m$ fading [21], [22]. Consequently, the channel power gains $|h_j|^2$, $j \in \{p, s, e\}$ are Gamma distributed random variables (RVs) with average power $\Omega_j$ and integer shape parameter $m_j \geq 1$ [23].

Hereby, the BS employs superposition coding to combine two independent unit energy signals $x_p$ and $x_s$ of PU and SU, respectively, as $x = \sqrt{\alpha_p} P x_p + \sqrt{\alpha_s} P x_s$, where $P$ is the total power at the BS and $\alpha_p$ and $\alpha_s$ are the power allocation coefficients such that $\alpha_p + \alpha_s = 1$. Depending upon the locations of PU and SU, we assume $|h_p|^2 < |h_s|^2$. Thus, the received signal at PU and SU can be compactly written as

$$y_j = h_j (\sqrt{\alpha_p} P x_p + \sqrt{\alpha_s} P x_s) \sqrt{G_{b,m} G_{j,m} \psi d_{j}^{-\alpha} + \eta_j},$$

where $j \in \{p, s\}$, $G_{b,m}$, $G_{p,m}$, and $G_{s,m}$ are directional antenna gains at BS, PU, and SU, respectively, $\psi = \left(\frac{c}{\pi f}ight)^2$ is path loss at unit distance, $c$ is the speed of light, and $f$ is the mmWave frequency. Further, $d_p$ and $d_s$ are the distances from BS to PU and BS to SU, respectively, and $\alpha$ is the path-loss exponent. $\eta_p$ and $\eta_s$ represent additive white Gaussian noise (AWGN) random variables distributed as circularly symmetric complex normal $CN(0, \sigma^2)$. From (2), the signal-to-interference-plus-noise ratio (SINR) at PU to decode $x_p$ can be expressed by replacing $j$ with $p$ in (3).

$$\Lambda_{x_p}^p = \frac{|h_p|^2 \alpha_p G_{b,m} G_{j,m} \psi d_{j}^{-\alpha}}{|h_j|^2 \alpha_s G_{b,m} G_{j,m} \psi d_{j}^{-\alpha} + \sigma^2_p}.$$  

Further, according to (2), the successive interference cancellation (SIC) receiver at SU first decodes the $x_p$ and then removes this signal from the observation to detect its own signal $x_s$. Thus, the SINR at SU to decode $x_p$ first can be given by replacing $j$ with $s$ in (3). After SIC, the signal-to-noise ratio (SNR) at SU to decode its signal $x_s$ is given by

$$\Lambda_{x_s}^s = \frac{|h_s|^2 \alpha_s G_{b,m} G_{j,m} \psi d_{j}^{-\alpha}}{\sigma^2_s}.$$  

Moreover, the observation at the Eve can be given by

$$y_e = h_e (\sqrt{\alpha_p} P x_p + \sqrt{\alpha_s} P x_s) \sqrt{G_{b,m} G_{c,m} \psi d_{e}^{-\alpha} + \eta_e},$$

where $G_{b,s}$ and $G_{c,m}$ are antenna gains at BS and Eve, respectively, $d_e$ is the distance between BS and Eve, and $\eta_e$ denotes AWGN $CN(0, \sigma^2_e)$ at Eve. Now, Eve can intercept either of the two end-users’ information by aligning itself to the main beam. Hence, using (5), the SINR to intercept the information of PU and SU can be given as

$$\Lambda_{x_j}^e = \frac{|h_j|^2 \alpha_j P G_{b,m} G_{c,m} \psi d_{j}^{-\alpha}}{|h_e|^2 \alpha_j P G_{b,m} G_{c,m} \psi d_{j}^{-\alpha} + \sigma^2_e},$$

where $j, \hat{j} \in \{p, s\}$ with $j \neq \hat{j}$. Hereafter, without losing generality, we assume that Eve particularly intends to intercept the information of PU. The analysis can be directly extended for the case of Eve intercepting the SU’s information.
III. NOMA POWER ALLOCATION STRATEGIES

In this section, we first briefly introduce the conventional fixed power allocation strategy and then present the proposed user-centric performance-based power allocation strategy for the considered NOMA-enabled downlink mmWave network.

A. Fixed power allocation strategy

In this strategy [10], the coefficients $\alpha_p$ and $\alpha_s$ are chosen randomly while satisfying the conditions $\alpha_p + \alpha_s = 1$. Such a strategy may not be useful when one of the end-users is a priority user demanding certain QoS.

B. User-centric performance-based power allocation strategy

In this strategy, power allocation coefficients are chosen to guarantee certain QoS of a targeted end-user.

1) Instantaneous CSI-assisted power allocation strategy: Since the PU is a targeted priority cell-edge user, it is intuitive to guarantee its QoS. For this, we impose the constraint to satisfy the achievable rate at the PU as [14]

$$\log_2 (1 + \Lambda_p^x) \geq R_p, \quad (7)$$

where $R_p$ is the rate at PU to successfully decode $x_p$. On solving (7), we can obtain $\alpha_s$ analytically as

$$\alpha_s = \max \left(0, \frac{1}{A}(AP|h_p|^2 - \gamma_{th,s}^p)/(AP|h_p|^2(1 + \gamma_{th}^p)) \right), \quad (8)$$

where $A = G_b,mG_p,m\psi d^{-\alpha}$ and $\gamma_{th}^p = 2\rho_p - 1$. Note that strategy in (8) requires acquisition of the instantaneous CSI of pertaining links for power allocation which adds to the system overhead and thus complexity.

2) Proposed Average CSI-assisted power allocation strategy: In this strategy, the QoS of PU can be guaranteed when its OP is kept below certain pre-defined threshold $\xi_{th}$, i.e., $\mathbb{P} \left[ \log_2 (1 + \Lambda_p^x) \leq R_p \right] \leq \xi_{th}$ which using (3) yields

$$\mathbb{P} \left[ \frac{A\alpha_s P|h_p|^2 + \sigma_p^2}{A\alpha_s P|h_p|^2} \leq \xi_{th} \right] \leq \xi_{th}, \quad (9)$$

Note that in (9), the channel gain $|h|^2$ is an ordered random variable. So, by applying order statistics, its cumulative distribution function (CDF) can be obtained as $F_{|h|^2}(z) = 2F_{|\tilde{h}|^2}(z) - (F_{|\tilde{h}|^2}(z))^2$, where $|\tilde{h}|^2$ is an unordered random variable. Using this, we can evaluate (9) with the aid of multinomial theorem [24], [25] to get

$$1 - \exp \left( - \frac{2m\gamma_{th}^p\sigma_p^2}{\alpha_s \lambda P} \sum_{l=0}^{m-1} \beta_{l,2} \left( \frac{m\gamma_{th}^p\sigma_p^2}{\lambda P} \right)^l \right) \leq \xi_{th}, \quad (10)$$

where $\lambda = 1 - \alpha_s (\gamma_{th,s}^p + 1)$ and coefficients $\beta_{l,2}$ are obtained as $\beta_{l,2} = \sum_{i=1}^{m-l} \beta_{i,2} \frac{1}{(m-l)!} \beta_{0,0}$, $\beta_{0,0} = 1$, $\beta_{l,1} = 1/l!$, $\beta_{1,2} = 2$, $\beta_{l,2} = 1$, $\beta_{0,0} = 0$, otherwise. Herein, (10) is valid for the condition $\rho_p < \alpha_s \gamma_{th,s}^p$. For a fixed $\xi_{th}$, the power allocation coefficient can be obtained by numerically solving (10) with respect to $\alpha_s$. However, for a special case when $m = 1$, $\alpha_s$ can be obtained in closed-form as

$$\alpha_s = \frac{1}{1 + \gamma_{th}^p} \left( 1 + \frac{2\gamma_{th}^p\sigma_p^2}{\lambda P \log_e (1 - \xi_{th})} \right). \quad (11)$$

We emphasize that the aforementioned power allocation strategy relies upon the average CSI only, which is relatively stable with limited feedback overhead.

IV. SECRECY-RELIABILITY PERFORMANCE TRADE-OFF

In this section, we analyze the IP and OP for characterizing the security and reliability performance of the considered system.

A. Intercept probability

IP can be defined as the event when the capacity at Eve becomes higher than the rate difference between the user target rate and secrecy rate. In other words, it signifies that the perfect secrecy is not achievable, and an intercept event has occurred. Thus, it can be expressed for PU as [26]

$$\mathbb{P}_{\text{int, } P_i} = \mathbb{P} \left[ \log_2 (1 + \Lambda_p^x) > R_p - R_o \right] \quad (12)$$

$$= 1 - \mathbb{P} \left[ \Lambda_p^x \leq \gamma_{th,e}^p \right],$$

where $\gamma_{th,e}^p = 2R_p - R_o - 1$ with $R_o$ be the secrecy rate. Based on (6), we can evaluate (12) to obtain

$$\mathbb{P}_{\text{out, } P_i} = \sum_{n=0}^{m-1} \frac{1}{n!} \left( \frac{m_e}{\Omega_e} \right)^n \left( \frac{\gamma_{th,e}^p \sigma_e^2}{\Omega_e \beta_{th,e} \sigma_e^2} \right)^n \exp \left( - \frac{m_e}{\Omega_e \beta_{th,e} \sigma_e^2} \right), \quad (13)$$

where $\beta = G_b,sG_e,m\psi d^{-\alpha}$. Similarly, the IP at the SU can be derived. It is the same as (13) whereby $\alpha_p, \gamma_{th,e}^p$, and $\gamma_{th,e}^p$ are replaced with $\alpha_s, \omega_p$, and $\gamma_{th,e}^p$. Herein, $\gamma_{th,e}^p = 2R_p - R_s - 1$ containing $R_s$ as the target rate at SU. We further simplify the derived IP in (13), at high SNR ($P \rightarrow \infty$) as

$$\mathbb{P}_{\text{int, } P_i} \approx 1 - \frac{1}{\Gamma(m_e + 1)} \left( \frac{m_e \gamma_{th,e}^p \sigma_e^2}{\Omega_e \beta_{th,e} \sigma_e^2} \right)^{m_e}, \quad (14)$$

where the approximation $\Upsilon(m, x) \approx x_m^m$ has been applied. Here, $\Upsilon(., .)$ represents the lower incomplete gamma function.

B. Outage probability

When the capacity of the main channel between the transmitter and the legitimate receiver falls below a target rate, it is impossible for the receiver to successfully decode the source message and an outage event occurs. For PU, OP is given as

$$\mathbb{P}_{\text{out, } P_i} = \mathbb{P} \left[ \log_2 (1 + \Lambda_p^x) \leq R_p \right], \quad (15)$$

which can be readily evaluated using (10) to get

$$\mathbb{P}_{\text{out, } P_i} = 1 - \exp \left( - \frac{2m\gamma_{th}^p\sigma_p^2}{\alpha_s \lambda P} \sum_{l=0}^{m-1} \beta_{l,2} \left( \frac{m\gamma_{th}^p\sigma_p^2}{\lambda P} \right)^l \right), \quad (16)$$

Further, at high SNR, it can be approximated as

$$\mathbb{P}_{\text{out, } P_i} \approx \frac{2}{\Gamma(m_e + 1)} \left( \frac{m \gamma_{th,e}^p \sigma_e^2}{\Omega_e \beta_{th,e} \sigma_e^2} \right)^{m_e}. \quad (17)$$
Likewise, the OP of SU can be obtained as
\[
P_{\text{out, SU}} = P\left[\log_2(1 + \Lambda_s) \leq \mathcal{R}_s\right] = P\left[h_s^2 \leq \frac{\gamma_{th}^o s^2}{\alpha s PC}\right],
\]
where \( C = G_{b,m} G_{s,m} d_s^\alpha \) and \( \gamma_{th}^o = 2^{\mathcal{R}_s} - 1. \) In (18), \( |h_s|^2 \) is an ordered random variable with its CDF as \( F_{|h_s|^2}(x) = (F_{|h_s|^2}(x))^2 \), where \( F_{|h_s|^2}(x) \) is an unordered random variable. Now, upon evaluating (18), we obtain \( P_{\text{out, SU}} \) as
\[
P_{\text{out, SU}} = \frac{2}{q} \sum_{q=0}^{\infty} \sum_{k=0}^{(q-1)} \left(\frac{q}{q}\right)^k \frac{(m_s)^k}{(m_s - 1)} \right)
\times \exp \left(-\frac{q m_s \gamma_{th}^o s^2}{\alpha s PC}\right).
\]
where the coefficients \( \beta_{k,q} \) are calculated as
\[
\beta_{k,q} = \frac{\prod_{i=k}^{m_s-1} \Gamma(q)}{\Gamma(m_s)} \beta_{0,0} = 1, \quad \beta_{k,1} = 1/k!, \quad \beta_{1,q} = q, \quad \Gamma(q) = 1 \quad \text{for} \quad 0 \leq q \leq (q - 1)(m_s - 1), \quad \text{and} \quad \Gamma(q) = 0 \quad \text{otherwise}.
\]
Moreover, at high SNR, (19) can be approximated as
\[
P_{\text{out, SU}} \approx \left(\frac{m_s \gamma_{th}^o s^2}{\Omega_s PC}\right)^2.
\]

V. NOMA/OMA MODE SELECTION

Importantly, NOMA cannot always guarantee a superior performance as compared to conventional OMA [27]. Therefore, we formulate a condition so that the secrecy performance of NOMA is guaranteed to be superior to OMA. Since we aim to ensure the QoS and the secrecy performance of PU, its IP should be less for NOMA than for the OMA, i.e.,
\[
P_{\text{int,PU}} \leq P_{\text{OMA}}^{\text{out,PU}},
\]
where \( P_{\text{int,PU}} \) is given by (13). The IP \( P_{\text{OMA}}^{\text{out,PU}} \) for OMA case can be obtained as
\[
P_{\text{OMA}}^{\text{out,PU}} = P\left[(1/2) \log_2(1 + \Lambda_{\text{tp},\text{OMA}}) > \mathcal{R}_p - \mathcal{R}_s\right],
\]
where pre-log factor 1/2 accounts for the two time-slot transmission in OMA. The SINR \( \Lambda_{\text{tp},\text{OMA}} \) can be obtained by substituting \( \alpha_p = 1, \alpha_s = 0 \) in (6). On solving (22), we get
\[
P_{\text{OMA}}^{\text{out,PU}} = \frac{m_s - 1}{2} \sum_{r=0}^{m_s - 1} \left(\frac{m_s \gamma_{th}^o s^2}{\Omega_s PC}\right)^r.
\]
with \( \gamma_{th, e}^o = 2^{(\mathcal{R}_e - \mathcal{R}_s)} - 1. \) Now using (13) and (23) in (21), we obtain the condition on \( \alpha_s \) as
\[
1 + \frac{\gamma_e}{\gamma_{th, e}} \left(1 - \frac{\gamma_{th, e}}{\gamma_{th, e}}\right) \leq \alpha_s < \frac{1}{1 + \gamma_{th, e}}.
\]
Clearly, if the power allocation coefficients are set as per (24), the secrecy performance of NOMA is always better than OMA. Note that the \( \alpha_s^* \) solely depends on the target secrecy rates and independent of the other system parameters.

Remark: The condition, given in (10) or (11), needs to be satisfied to ensure the reliability of PU. Whereas, to guarantee its secrecy performance, the condition in (24) should be satisfied. As a result, to ensure the security and reliability of PU simultaneously, both these conditions must be fulfilled, which may not be feasible due to the dependence upon the various system parameters. Consequently, there exists an SRPT to perform the NOMA power allocation satisfactorily.

VI. NUMERICAL AND SIMULATION RESULTS

For numerical analysis, we set various system parameters as \( f = 28 \) GHz, \( G_{b,m} = G_{s,m} = G_{e,m} = 16 \) dB, \( G_{b,s} = 10 \) dB, \( \Omega_s = 1, \mathcal{R}_p = 0.5, \mathcal{R}_s = 1, \mathcal{R}_o = 0.1, \sigma_i = 1, \) \( d_p = 10 \) m, \( d_s = 15 \) m, and \( d_e = 30 \) m.

Fig. 2 plots the OP versus SNR for PU and SU. The analytical and asymptotic curves are well-aligned with simulations. Clearly, when \( m_p (m_s) \) increases, the OP improves for PU (SU). It follows due to better channel conditions for larger values of \( m_p (m_s) \). The steeper slope of asymptotic OP curve for SU reveals its higher performance gain relative to PU.

Fig. 3 plots the variation of the power allocation factor versus SNR as per Sec. III. Herein, we consider three different tolerable OP thresholds to plot the curves. Note that there is a feasible upper cut-off value of \( \alpha_s \) at certain SNR beyond which effective communication is not supported for a given threshold. For the three OP thresholds, it can be observed that the upper cut-off values of \( \alpha_s \) are \( 0.2621, 0.4144, \) and \( 0.4002 \) at SNRs 25 dB, 35 dB, and 45 dB, respectively.

Fig. 4 plots the curves between IP and OP of PU for variable \( d_e \). It reveals an SRPT, that is, improving the IP (i.e., secrecy) results in deterioration of OP for PU (i.e., reliability). Thus, a balanced operating point may be chosen based on SRPT of the system. Besides, the prevailing SRPT can also be inferred based on the arguments given in Sec. V.

Fig. 5 plots IP and \( \alpha_s \) to compare the secrecy performance of NOMA with OMA. We observe that a feasible value of \( \alpha_s \) can be obtained to guarantee the secrecy performance of PU with NOMA better than that with OMA. This fact can be observed through the cross-over point (\( \alpha_s^* \)) of the curves plotted for NOMA and OMA schemes. As long as \( \alpha_s < \alpha_s^* \) is set, the NOMA realizes a superior performance gain. Whereas, for \( \alpha_s < \alpha_s^* \), NOMA exhibits inferior performance compared to OMA. In such case, the mode switching from NOMA to
decreases as OMA can be initiated by the system. Note that the value of $\alpha_*$ decreases as $R_p$ increases. The value of $\alpha_*$ can be analytically obtained in the range specified by (24).

VII. CONCLUSION

We investigated the SRPT for a NOMA-based mmWave network. Here, we considered a system scenario in which an eavesdropper attacks to tap the secure information of NOMA users served by a mmWave BS. A low-complexity average CSI-based power allocation method was proposed to ensure the reliability of targeted end-user for certain information secrecy. We derived the closed-form expressions for the OP and IP of eavesdropper corresponding to a targeted user to analyze the SRPT. We obtained a design condition for the power allocation coefficient which ensures the outperformance of NOMA over OMA. It was observed that, for a given OP threshold at a certain SNR, effective communication is not supported beyond a cut-off power allocation coefficient. Finally, the SRPT analysis revealed that an operating region can be established to balance between the secrecy and reliability performance.

ACKNOWLEDGMENT

This work was partially supported by the FNR-funded project CORE 5G-Sky (Grant C19/IS/13713801). This work was also supported in part by the Science and Engineering Research Board (SERB), Department of Science and Technology, Govt. of India, under Project SRG/2019/000979.

REFERENCES

[1] L. Wang, Y. L. Che, J. Long, L. Duan, and K. Wu, “Multiple access mmWave design for UAV-aided 5G communications,” IEEE Wireless Commun., vol. 26, no. 1, pp. 64-71, Feb. 2019.
[2] Z. Ding, P. Fan, and H. V. Poor, “Random beamforming in millimeter-wave NOMA networks,” IEEE Access, vol. 5, pp. 7667-7681, 2017.
[3] D.-D. Tran, S. K. Sharma, S. Chatzinotas, I. Woungang, and B. Ottersten., “Short-packet communications for MIMO NOMA systems over Nakagami-m fading: BLER and minimum blocklength analysis,” IEEE Trans. Veh. Technol., vol. 70, no. 4, pp. 3583-3598, Apr. 2021.
[4] D. Zhang et al., “Capacity analysis of NOMA with mmWave massive MIMO systems,” IEEE J. Sel. Areas Commun., vol. 35, no. 7, pp. 1606-1618, Jul. 2017.
[5] Z. Ding et al., “NOMA meets finite resolution analog beamforming in massive MIMO and millimeter-wave networks,” IEEE Commun. Lett., vol. 21, no. 8, pp. 1879-1882, Aug. 2017.
[6] B. Wang et al., “Spectrum and energy-efficient beamforming in millimeter-wave NOMA: MMF-NOMA for millimeter-wave communications using lens antenna array,” IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2370-2382, Oct. 2017.
[7] K. Belbase, C. Tellambura, and H. Jiang, “Coverage analysis of cooperative NOMA in millimeter wave networks,” IEEE Commun. Lett., vol. 23, no. 12, pp. 2154-2158, Dec. 2019.
[8] Y. Wu et al., “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679-695, Apr. 2018.
[9] S. Solanki and P. K. Upadhyay, “Secure underlay cognitive relay networks in presence of primary user’s interference,” in Proc. IEEE VTC Spring, Sydney, NSW, 2017.
[10] J. Chen, L. Yang, and M.-S. Alouini, “Physical layer security for cooperative NOMA networks,” IEEE Trans. Veh. Technol., vol. 67, no. 5, pp. 4645-4649, May 2018.
[11] Z. Xiang et al., “Secure transmission design in HARQ assisted cognitive NOMA networks,” IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 2528-2541, Jan. 2020.
[12] X. Tian, Q. Liu, Z. Wang, and M. Li, “Secure hybrid beamformers design in mmWave wiretap systems,” IEEE Syst. J., vol. 14, no. 1, pp. 548-559, Mar. 2020.
[13] N. Rupasinghe et al., “Enhancing physical layer security for NOMA transmission in mmWave drone networks,” 52nd Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 2018.
[14] Y. Song et al., “Secure transmission in mmWave NOMA networks with cognitive power allocation,” IEEE Access, vol. 7, pp. 76104-76119, 2019.
[15] F. Zhao et al., “Secure energy efficiency transmission for mmWave-NOMA system,” IEEE Systems J., vol. 15, no. 2, pp. 2226 - 2229, June 2021.
[16] X. Sun, W. Yang, and Y. Cai, “Secure communication in NOMA-assisted millimeter-wave SWIPT UAV networks,” IEEE Internet of Things J., vol. 7, no. 3, pp. 1884-1897, March 2020.
[17] S. K. Sharma and X. Wang, “Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions,” IEEE Commun. Surveys Tut., vol. 22, no. 1, pp. 426-471, May. 2019.
[18] P. Korrai et al., “A RAN resource slicing mechanism for multiplexing of eMBB and URLLC services in OFDMA based 5G wireless networks,” IEEE Access, vol. 8, pp. 45674-45688, Mar. 2020.
[19] “Study on non-orthogonal multiple access (NOMA) for NR,” 3GPP, Tech. Rep. 38.812, Dec. 2018.
[20] B. Makki, K. Chitti, A. Behravan, and M.-S. Alouini. “A survey of NOMA: Current status and open research challenges,” IEEE Open J. Commun. Soc., vol. 1, pp. 179-189, Jan. 2020.
[21] H. Ding, D. B. da Costa, J. Coon, and Y. Chen, “Relay when blocked: A hop-by-hop mmWave cooperative transmission protocol,” IEEE Commun. Lett., vol. 22, no. 9, pp. 1894-1897, May 2018.
[22] L. Tiebaldiyeva et al., “Device-to-device mmWave communication in the presence of interference and hardware distortion noises,” IEEE Commun. Lett., vol. 23, no. 9, pp. 1607-1610, Sep. 2019.
[23] S. Solanki et al., “Performance analysis of cognitive relay networks with RF hardware impairments and CEEs in the presence of primary users interference,” IEEE Trans. Cogn. Commun. Netw., vol. 4, no. 2, pp. 406-421, Jun. 2018.
[24] J. M. Moualeu et al., “Transmit antenna selection in secure MIMO systems over α-μ fading channels,” IEEE Trans. Commun., vol. 67, no. 9, pp. 6483-6498, Sep. 2019.
[25] S. Solanki et al., “Performance analysis of piece-wise linear model of energy harvesting-based multiuser overlay spectrum sharing networks,” IEEE Open J. Commun. Soc., vol. 1, pp. 1820-1836, Nov. 2020.
[26] Y. Zou, M. Sun, J. Zhu, and H. Guo, “Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks,” IEEE Trans. Wireless Commun., vol. 17, no. 12, pp. 8444-8456, Dec. 2018.
[27] P. K. Sharma and D. I. Kim, “UAV-enabled downlink wireless system with non-orthogonal multiple access,” in Proc. IEEE Globecon Workshops, Singapore, Dec. 2017, pp. 1-6.