Secure mm-Wave communications with imperfect hardware and uncertain eavesdropper location

Saeed Mashdour¹ | Majid Moradikia¹ | Phee Lep Yeoh²

¹School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran
²School of Electrical and Information Engineering, The University of Sydney, Sydney, Australia

Correspondence
Saeed Mashdour, School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran.
Email: smashdour@gmail.com

Abstract
This article examines the secrecy performance of millimeter-wave (mm-Wave) communications with imperfect hardware and uncertain eavesdropper (Eve) location. We consider a multiple-antenna source communicating with a single-antenna destination using masked beamforming to transmit the information signals with artificial noise (AN) in the presence of a passive Eve. For this system, we derive new expressions for the secrecy outage probability (SOP) and secrecy throughput with mm-Wave multipath propagation under slow-fading channel conditions and hardware imperfections. Based on this, optimal power allocation (OPA) solutions are derived for the information and AN signals aimed at minimizing the SOP and maximizing the secrecy throughput. Our results reveal that it is non-trivial to achieve an OPA solution for the general scenario of imperfect hardware. We also highlight that our proposed masked beamforming with OPA scheme significantly enhances the secrecy throughput compared with the benchmark schemes of maximal-ratio transmission and equal power allocation.

1 | INTRODUCTION

The ubiquity of wireless technology has led to an enormous amount of sensitive and confidential information being transmitted via the open wireless medium. Due to the randomness and broadcast nature of electromagnetic waves, the security of wireless communications conventionally implemented above the physical layer via key-based cryptography¹ is becoming increasingly challenging. Recently, the so-called physical layer security (PLS) approach, in which the dynamic characteristics of wireless links are intelligently exploited has attracted significant attention in the literature.²,³ For instance, unmanned aerial vehicle (UAV) networks with covert communications for transmission with location uncertainty of the transmitter or receiver was considered in Reference 4 such that the information is not detected by a ground warden. Also, PLS of a UAV network for transmission of confidential information from a base station to multiple receivers utilizing a UAV jammer in presence of multiple eavesdroppers (Eves) was studied in Reference 5.

PLS of overlay device-to-device untrusted relaying in the presence or absence of a friendly jammer was comprehensively analyzed in Reference 6 and secrecy performance of cellular multi-user decode-and-forward based two-way relaying networks was investigated in Reference 7 where a multi-antenna base station communicates bi-directionally with several users by the aid of decode-and-forward relay(s) under the existence of a multi-antenna passive eavesdropper. In recent years, massive multiple-input multiple-output systems have come into prominence due to the significant perfor-
formance gains in terms of security, spectral efficiency, and energy saving. Typically, multiple antenna transmitters have been considered to transmit narrow directional beams towards the legitimate destination to increase the received signal power relative to the eavesdropper based on known channels state information (CSI). When the exact CSI of Eve is unknown, the transmitter can broadcast the information signal together with artificial noise (AN) to degrade Eve’s channel. The secrecy performance of AN-aided transmission has been investigated for both fast and slow-fading channels. For fast-fading channels, the channel coherence time is much shorter than the codeword length, thus beamforming and optimal power allocation (OPA) strategies are based on the ergodic secrecy rate. However, in the case of slow-fading channels, outage-based formulations are more suitable. Along this line, the OPA strategy towards the goal of the secrecy outage probability (SOP) minimization is studied in References 15,16. In recent years, different literatures have used PLS in the context of high-frequency millimeter-wave (mm-Wave) bands, that is, 30-300 GHz. In Reference 20, the ray-cluster channel model has been used which is known to accurately model the multipath propagation in mm-Wave systems. However, only the works of References 18,19,21 have analyzed the PLS using the ray-cluster channel in mm-Wave communication systems. Another important consideration in wireless systems is the impact of hardware impairments, due to I/Q imbalance, oscillator phase noise (PN), high power amplifier nonlinearities, and quantization errors. It was found in References 26,27 that even after applying transmitter calibration and compensation algorithms at the receiver, there still remains a combination of multiplicative PN and distortion noises at both the transmitter and receiver. Recently, the PLS design with imperfect hardware has been investigated in References 14,28,29 for microwave channels. For mm-Wave systems, the effect of imperfect hardware is intensified due to several reasons. First, the high carrier frequency leads to larger multiplication factors which results in phase noise amplification. Also, a bank of phase shifters is needed to connect to high or massive number of antennas to control the hardware cost and power consumption. Furthermore, mm-Wave systems are more sensitive to angular mismatches due to strong directionality provided by large antenna numbers. Thus, it is necessary to consider hardware imperfection in the design and analysis of mm-Wave communication systems. Millimeter wave systems are known to provide enhanced secrecy against eavesdroppers due to the directional signal beams from highly directional phased-array antennas. However, signal beam reflections from ambient reflectors and eavesdropping strategies using skillfully designed beam exploration have created significant possibilities for eavesdroppers to attack the confidential information, so that even only one eavesdropper could intercept transmitted signals successfully. As such, we are motivated in this article to consider the impact of eavesdropping in the PLS of mm-Wave systems using the ray-cluster model with imperfect hardware and slow-fading channels. To do so, we make the practical assumptions that exact CSI of Eve is unavailable, and the distortion noise follows a Gaussian distribution based on the aggregate contribution of multiple hardware impairments. We assume Eve is randomly located and, based on the slow-fading assumption, there exists a suspicious eavesdropping region where Eve is likely to be located around the source and destination. For this system, we design a new secure AN masked beamforming and separately analyze the OPA aimed at SOP minimization and secrecy throughput maximization. The impact of hardware imperfection results in a more general expression for the mm-wave OPA compared with the ideal hardware case considered in Reference 18. It is noted here that due to the larger free-space loss and large number of the implemented antennas in mm-Wave wireless communication systems, perfect knowledge of CSI is difficult to achieve. In such situations, beam training via spatial scanning is a common approach to achieve large beamforming gains by adaptive aligning of the transmitter and the receiver beams. Spatial scanning utilizes exhaustive and hierarchical search strategies through the codebooks that cover the scanning space to determine the best beam which aligns with the dominant paths for communications. The main contributions of the article are summarized as follows:

- The generalized system model for transceiver hardware imperfections is detailed after presenting the discrete angular domain channel (DADC) model for our mm-wave system constructed by spatially resolvable paths.

- We derive the signal-to-noise-plus-distortion ratios (SNDRs) at the Eve and the legitimate destination with secure AN masked beamforming. We also discuss the impact of hardware imperfections in the high-signal-to-noise ratio (SNR) regime.

- We derive a new closed-form expression for the SOP of mm-wave systems with AN and imperfect hardware when the exact eavesdropper location is unknown. Based on this, we formulate the OPA factor between the source and the destination such that the SOP is minimized.

- We also derive the OPA which maximizes the secrecy throughput under a SOP constraint. We also present high SNR analysis to identify the impact of hardware imperfection on the secrecy performance and OPA.
• We show in our analytical and experimental results that imperfect hardware results in more power allocated to the AN signal to boost the secrecy of the system. We also show that the secrecy performance with AN is improved in comparison with traditional maximum ratio transmitting (MRT) beamforming.

Our derived solutions characterize the decrease in secrecy performance of mm-wave systems with imperfect hardware compared to the ideal hardware case. We also highlight that AN beamforming can protect against eavesdropper interception in mm-wave systems with imperfect hardware.

2 | SIGNAL AND SYSTEM MODEL

In this section, we detail the mm-Wave channel model, transceiver hardware imperfections, and dynamic on-off transmission scheme considered in our system model. We assume a multi-antenna source (S) equipped with an array of $M$ antennas communicates with a single antenna destination $(D)$, while a single antenna Eve $(E)$ attempts to eavesdrop the transmitted information. We assume that instantaneous CSI of $D$ is perfectly known at $S$ but the CSI of $E$ is unknown. We consider slow-fading in which the complex channel gains in a single frame are unchanged although they change independently from one frame to another.

2.1 | Ray-cluster channel model

Due to the sparse scattering and multipath propagation, the mm-Wave channel is well-modeled using a ray-cluster based spatial model, where the channel is represented by multiple clusters each of which comprises several paths. Since it is possible to concentrate the mm-Wave transmission power in a particular cluster, the channel is assumed to have a single cluster. We apply a DADC model for the spatially resolvable multipaths\cite{18,37} where the angular domain at a fixed spatial model, where the channel is represented by multiple clusters each of which comprises several paths. Since it is possible to concentrate the mm-Wave transmission power in a particular cluster, the channel is assumed to have a single cluster. We apply a DADC model for the spatially resolvable multipaths\cite{18,37} where the angular domain at a fixed angular spacing of $\frac{\lambda}{L}$ is uniformly sampled at the transmitter. The length of the mm-Wave transmit antenna array is denoted by $\Delta = \frac{\lambda}{2}$ which determines the angular domain resolvability. Antenna spacing is also denoted by $\Delta = \frac{\lambda}{2}$ where $\lambda$ is the wavelength. Then, the DADC model can be represented by a unitary matrix $W \in \mathbb{C}^{M \times M}$ whose columns form an orthogonal basis of the transmitted signal space defined as

$$W \triangleq [R(\varphi_1), R(\varphi_2), \ldots, R(\varphi_M)],$$

where $\varphi_i \triangleq \frac{1}{L} \left(i - 1 - \frac{M-1}{2}\right)$ for $i = 1, 2, \ldots, M$ and $R(\varphi_i) \triangleq \frac{1}{\sqrt{M}} \left[1, e^{-j2\pi \frac{2}{\lambda}}, \ldots, e^{-j(M-1)2\pi \frac{2}{\lambda}}\right]^T$ is the normalized array response (steering vector) at the azimuth angle of departure (AOD) $\theta_i = \sin^{-1} \varphi_i$. Assuming AOD of all paths distributed within the angular range $[\theta_{\text{min}}, \theta_{\text{max}}]$, where $\{\theta_{\text{min}}, \theta_{\text{max}}\} \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, we will have $\varphi_i \in [\sin \theta_{\text{min}}, \sin \theta_{\text{max}}]$. Thus, the DADC model is described as

$$h \triangleq \sqrt{\frac{M \alpha}{N}} g W^H,$$

where $g \triangleq [g_1, g_2, \ldots, g_M]$ is the complex channel gain vector. If $\varphi_i \in [\sin \theta_{\text{min}}, \sin \theta_{\text{max}}]$, $g_i$ is considered as a complex Gaussian coefficient with zero mean and unit variance, otherwise it will be zero. We also denote $\alpha$ as the average path loss between the transmitter and the receiver, and $N$ as number of the spatially resolvable paths $(N < M)$. Based on (2), $h_D \triangleq \sqrt{\frac{M \alpha_D}{N_D}} g_D W^H$ and $h_E \triangleq \sqrt{\frac{M \alpha_E}{N_E}} g_E W^H$ are the $S \rightarrow D$ and $S \rightarrow E$ channels respectively, where $\alpha_D$ and $\alpha_E$ are the corresponding path losses, $g_D \in \mathbb{C}^{1 \times M}$ and $g_E \in \mathbb{C}^{1 \times M}$ denote the relevant complex gains, $N_D$ and $N_E$ are numbers of spatially resolvable paths in the destination and the eavesdropper channels with $N_D < M$, $N_E < M$. The basis vectors of the destination and eavesdropper are denoted by $I_{D_i}$ for $i = 1, 2, \ldots, N_D$ and $I_{E_i}$ for $i = 1, 2, \ldots, N_E$, respectively. As shown in Figure 1, the destination’s resolvable paths are selected from the set $\Xi_D \triangleq \{I_D | I_D i \in \mathbb{Z}^+, I_D i \in [1, M], I_D_1 < I_D_2 < \ldots < I_D_{N_D}\}$ while the eavesdropper’s resolvable path are selected from the set $\Xi_E \triangleq \{I_E | I_E i \in \mathbb{Z}^+, I_E i \in [1, M], I_E_1 < I_E_2 < \ldots < I_E_{N_E}\}$. We denote the common paths of $D$ and $E$ by the set $\Xi_C \triangleq \Xi_D \cap \Xi_E$. On the other hand, the set $\Xi_A \triangleq \Xi_E \setminus \Xi_D$ shows all the members in $\Xi_E$ but not in $\Xi_D$ and $\Xi_B \triangleq \Xi_D \setminus \Xi_E$ represents all the members in $\Xi_D$ but not in $\Xi_E$. Moreover, for a given matrix $B \triangleq [b_1, b_2, \ldots, b_m]$ and the set $\Xi \triangleq \{I | I i \in \mathbb{Z}^+, I i \in [1, m], I_1 < I_2 < \ldots < I_n, n \leq m\}$, the operator
\( \mathcal{S}(\mathbf{B}, \Xi) \) generates the matrix \( \mathbf{\tilde{B}} \triangleq [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_L] \) whose columns are selected from \( \mathbf{B} \) based on those indices which lie within \( \Xi \). Accordingly, we define \( \mathbf{\tilde{g}}_D \triangleq \mathcal{S}(\mathbf{g}_D, \Xi) \in \mathbb{C}^{1 \times N_D}, \mathbf{\tilde{g}}_E \triangleq \mathcal{S}(\mathbf{g}_E, \Xi) \in \mathbb{C}^{1 \times N_E}, \mathbf{\tilde{W}}_D \triangleq \mathcal{S}(\mathbf{W}, \Xi) \in \mathbb{C}^{M \times N_D} \) and \( \mathbf{\tilde{W}}_E \triangleq \mathcal{S}(\mathbf{W}, \Xi) \in \mathbb{C}^{M \times N_E} \) through which we can re-express the destination and eavesdropper channels as \( \mathbf{h}_D \triangleq \sqrt{\frac{M \alpha_D}{N_D}} \mathbf{\tilde{g}}_D \mathbf{\tilde{W}}_D^H \) and \( \mathbf{h}_E \triangleq \sqrt{\frac{M \alpha_E}{N_E}} \mathbf{\tilde{g}}_E \mathbf{\tilde{W}}_E^H \), respectively. In addition, defining \( N_{E-C} \triangleq N_E - N_C \) and \( N_{D-C} \triangleq N_D - N_C \), the corresponding complex channel gain vectors are defined as \( \mathbf{\tilde{g}}_E \triangleq \mathcal{S}(\mathbf{g}_E, \Xi) \in \mathbb{C}^{1 \times N_C}, \mathbf{\tilde{g}}_E \triangleq \mathcal{S}(\mathbf{g}_E, \Xi) \in \mathbb{C}^{1 \times N_E}, \mathbf{\tilde{g}}_D \triangleq \mathcal{S}(\mathbf{g}_D, \Xi) \in \mathbb{C}^{1 \times N_C}, \mathbf{\tilde{g}}_D \triangleq \mathcal{S}(\mathbf{g}_D, \Xi) \in \mathbb{C}^{1 \times N_E} \), as well. It is also noted that based on the intuitive results brought in Reference 18 we can reasonably assume that \( N_{D-C} > 0 \) and \( N_{E-C} > 0 \). Since \( \mathbf{g}_D \) and \( \mathbf{g}_E \) are uncorrelated and independent due to Gaussian distribution, we can also assume that \( \mathbf{\tilde{g}}_D \) and \( \mathbf{\tilde{g}}_E \) are uncorrelated and independent vectors.

### 2.2 Transceiver hardware imperfection

Figure 2 shows the statistical behavior of imperfect hardware at node \( i \in \{S, D\} \). We consider the ideal eavesdropper case, corresponding to the worst-case condition in terms of secrecy performance, where \( E \) does not have any hardware impairments. The distortion noises \( \eta_{\text{tx}} \) and \( \eta_{\text{rx}} \), respectively appeared at the transmitter of \( S \) and receiver of \( D \) as a consequence of hardware imperfection, causes a mismatch between the desired and the actual transmitted signal. This noise is well-modeled by a Gaussian distributed random variable. We consider the same model as Reference 28 where
the variance of the distortion noise at the ith node is proportional to the signal power at the corresponding antenna. Accordingly

$$\eta_{tx} \sim \mathcal{CN}(0, k^2_{tx} E\{x^Hx\}), \quad \eta_{rx} \sim \mathcal{CN}(0, k^2_{rx} E\{|h_E|^2\})$$

(3)

where $x \in \mathbb{C}^{M \times 1}$ is the transmitted signal vector. The design parameters $k_{tx}$ and $k_{rx}$, so-called error vector magnitudes (EVMs), characterize the level of imperfections in the transmitter and receiver hardware, respectively. EVM determines the quality of radio frequency (RF) transceivers and is defined as the ratio of the average distortion magnitude to the average signal magnitude. Notably, the EVM measures the joint effect of different hardware imperfections and compensation algorithms and thus it can be measured directly in practice. $^{14,28}$ 3rd generation partnership project long-term evolution has EVM requirements in the range of $k_{tx}, k_{rx} \in [0.08, 0.175]$, where smaller values are needed to achieve higher spectral efficiencies.

### 2.3 Dynamic on-off transmission

To address the AN and MRT (as a special case of AN) cases in our slow-fading scenario, we adopt an on-off transmission protocol$^{16}$ at the source based on having the instantaneous CSI at the destination and no CSI of the eavesdropper. In the on-off transmission scheme, the transmitter decides to transmit or not based on its knowledge of the receiver’s channel so that the transmitter decides when to transmit according to the instantaneous CSI of the destination to prevent undesirable transmissions which incur capacity outages ($R_i > C_D$) or unacceptably high risk of secrecy outage ($C_E > R_e$) where $R_i$ is the codeword rate, $R_e$ is the redundancy rate required to decode the confidential information. $^{38}$ $Y_D$ and $Y_E$ denote the instantaneous received signal-to-interference-plus-noise ratios, $C_D \triangleq \log_2(1 + Y_D)$ and $C_E \triangleq \log_2(1 + Y_E)$ are the channel capacity of the destination and eavesdropper respectively. According to Reference 15 our on-off transmission scheme is an adaptive scheme where the encoder adaptively selects the transmitted codeword rate $R_i$, according to the instantaneous CSI of the destination’s channel. In this scheme, the destination only needs to send its instantaneous SNR $Y_D$ to the transmitter. $R_i$ is arbitrarily set close to $C_D$ which is the largest possible rate without incurring any decoding error at the destination. Let $G \triangleq \|\hat{g}_D\|^2$ represents the overall channel gain of the destination, that is, $G = \hat{G} + \hat{G}$ where $\hat{G} \triangleq \|\hat{g}_D\|^2, \hat{G} \triangleq \|\tilde{g}_D\|^2$ are the instantaneous gains of the common and non-common paths, respectively. Therefore, the source transmits only when $G \hat{\in} (G, \hat{G}) \in \mathbb{R}^2$ is in the transmission region $\xi \triangleq \{G \geq C_D \geq R_e\}$ satisfying the transmission constraint $C_D > R_e$ where $R_e \triangleq R_i - R_c$ is the confidential information rate for a given source codebook.

### 3 SECURE ARTIFICIAL NOISE MASKED BEAMFORMING

We propose a secure AN masked beamforming scheme based on the slow-fading SNDR at the destination. With hardware impairments, it is typically assumed that the distortion noise benefits the system security by degrading the received SNDR at $E$. However, in our ray-cluster channel model, the distortion is an isotropically distributed spatial noise and affects all paths at both $E$ and $D$. As previously mentioned, we assume that while perfect CSI of the destination is known, the exact CSI of the eavesdropper is unavailable at the source. Therefore, in the beamforming transmission design, we assume that partial CSI of the eavesdropper channel should be estimated based on the slow-fading assumption where the exact location of the eavesdropper is unknown but there exists an eavesdropping region around the source and destination. Therefore, we
propose to improve the secrecy performance by transmitting artificial interference towards the eavesdropper’s resolvable paths which do not include the $N_C$ common paths that overlap with the main channel. As such, a mixed version of information bearing signal and AN is transmitted such that the AN signal is in the null space of the destination’s resolvable paths to guarantee not to interfere with the destination’s paths.

**Remark 1.** (*i.i.d. Rayleigh fading channel*): In typical wireless systems with statistically independent Rayleigh fading channels, if the source has no knowledge of the eavesdropper situation, the AN is broadcasted in the null space of the legitimate channel which is known at $S$. This null space calculation involves the singular value decomposition whose complexity is significantly increased by large number of transmit antennas. However, as discussed above, in our case, specific propagation characteristic of mm-Wave channels assist us to transmit AN towards the eavesdropper’s resolvable paths excluding the $N_C$ common paths with the destination.

Let $s$ represent the unit power information signal, that is, $E[|s|^2] = 1$. As such, the signal vector transmitted by $S$ in our proposed scheme is $x = \sqrt{\tau P}f_1s + \sqrt{\left(1 - \tau P\right)/N_{E-C}}Fz$ where $P$ is total transmitted power, $f_1 \triangleq h_D^H||h_D||$ and $F \triangleq \mathcal{S}(\mathbf{W}, \mathbf{Z}_A) = [f_{A_1}, f_{A_2}, \ldots f_{A_{N_{E-C}}}] \in \mathbb{C}^{M \times N_{E-C}}$ with $E[F^HF] = I_{N_{E-C}}$ representing the AN beamforming matrix designed to null out the jamming signal $E[zz^H] = I_{N_{E-C}}$ at $D$, that is, $h_DF = 0$. The power allocation factor $\tau \in [0, 1]$ determines the power ratio for the information signal and the AN. Interestingly, substituting $\tau = 1$, MRT beamformer is achieved. Using the above definition, the masked beamforming matrix $F$ is acquired by only choosing specific columns from $\mathbf{W}$ corresponding to $\mathbf{Z}_A$. According to Figure 2, the received signals at $D$ and $E$ are

$$y_{D, AN} = \sqrt{\tau P}h_Df_1s + \sqrt{\left(1 - \tau P\right)/N_{E-C}}h_DFz + h_D\eta_s + n_D$$

$$y_{E, AN} = \sqrt{\tau P}h_Ef_1s + \sqrt{\left(1 - \tau P\right)/N_{E-C}}h_EFz + h_E\eta_s + n_E$$

where $n_D$ and $n_E$ are i.i.d. additive white Gaussian noise with zero-mean and variance $\sigma_n^2$, that is, $n_D \sim \mathcal{C}(0, \sigma_n^2)$ and $n_E \sim \mathcal{C}(0, \sigma_n^2)$. According to (4) and (5) after simple algebraic manipulations, the SNDR at $D$ and $E$ can be respectively formulated as

$$Y_{D, AN} = \frac{\tau d}{\tau e + 1}$$

$$Y_{E, AN} = \frac{\tau au}{(1 - \tau)bv + \tau cu + 1}$$

where $a \triangleq \frac{\beta DG}{\tilde{G}}$, $b \triangleq \frac{\beta D(1 + k^2_{tx})}{N_{E-C}}$, $c \triangleq k^2_{tx}a$, $d \triangleq \beta_DG$, $e \triangleq k^2_{int}$, $\beta_D \triangleq \frac{\rho\sigma_n^2}{\gamma_{int}\sigma_n^2}$, $\beta_E \triangleq \frac{\rho\sigma_n^2}{N_{E-C}\sigma_n^2}$, the aggregate level of impairments of all network is denoted by $k^2_{int} \triangleq k^2_{tx} + k^2_{tx}$ and the channel gains are $\sim \text{Gamma}(N_{D, 1})$, $\tilde{G} \sim \text{Gamma}(N_{C, 1})$, and $\tilde{G} \sim \text{Gamma}(N_{D-C, 1})$. Furthermore, defining $u \triangleq \left|\hat{g}_E\right|^2||\hat{g}_E^H||$, since $\hat{g}_E$ and the unit norm vector $\frac{\hat{g}_E}{||\hat{g}_E||}$ are both Gaussian and independent, we have $u \sim \text{exp}(1)$ as stated in Reference 37. We also define $v \triangleq ||g_EW^HF||^2$ with $v \sim \text{Gamma}(N_{E-C}, 1)$ and the term $g_EW^HF$ therein is equivalent to $\hat{g}_E$. It should also be remarked here that, $u$ and $v$ are independent because $u \in \mathbb{C}$ and $v \in \mathbb{C}$ and $\mathbb{C} \cap \mathbb{C} = \emptyset$.

**Remark 2.** (*High-SNR Regime*): To gain deeper insights, we consider (6) and (7) in the high transmit SNR regime. When the transmit power $P$ is sufficiently large, we find that $Y_{D, AN}$ approaches a constant ceiling $Y_{D, AN}^{\text{ap}} = \frac{1}{k_{int}}$ which only depends on the EVMs at the nodes, while the information leaked towards $E$ significantly depends on the power allocation factor $\tau$. This reveals that choosing $\tau$ is crucial for guaranteeing secrecy in our considered network. In addition, it is not possible to achieve some target secrecy rates due to the ceiling defined above, no matter how much large the value of transmit power $P$.

**Remark 3.** (*Ideal Hardware-Masked Beamforming*): For the special assumption of ideal hardware at the nodes, the SNDRs calculated in (6) and (7) can be simplified to the received SNRs in References 18, 21 given by

$$Y_{D, AN}^{\text{id}} \triangleq \tau d,$$
\[
Y_{E,AN}^{\text{id}}(\Delta) \triangleq \frac{N_{E-C} \tau u}{(1 - \tau) R_E V + N_{E-C}}, \tag{9}
\]

Comparing (8), (9) with (6), (7), it can be clearly seen that the terms \(re\) and \(rcu\) in (6) and (7), respectively, contribute to a more complicated expression for the non-ideal hardware SNDRs. Based on (6) and (7), we see that the distortion noises emitted by \(E\) results in interference at both \(E\) and \(D\), while the self-distortion noise at \(D\) only degrades the received SNDR at the legitimate destination. Thus, even though hardware imperfection can intrinsically confuse passive eavesdroppers, the secrecy performance is still degraded.

It is also worthy of mention that the eavesdropper's SNDR in both cases of ideal and non-ideal hardware, which were derived respectively in (7) and (9), is calculated based on the fact that \(\hat{g}_E \hat{g}_D^H = \bar{g}_E \bar{g}_D^H\) which is only achieved when the \(i\)th path is chosen from the common set \(\Xi_C\), that is, \(i \in \Xi_C\), \(\hat{g}_E \hat{g}_D^H \neq 0\). If there are no common paths between \(D\) and \(E\), that is, \(N_C = 0\), the array steering vectors within \(\hat{W}_D\) and \(\hat{W}_E\) will be orthogonal, resulting in \(Y_{E,AN} = 0\). Thus, it can be concluded that in the situation of \(N_C = 0\), the secrecy can be effectively guaranteed by using a simple beamformer which has low implementation complexity in contrast to other complicated precoder techniques at the multi-antenna transmitter.

It is also worthy of mention that if \(N_C\) is increased, \(\hat{G}\) in both the numerator and denominator of \(Y_{E,AN}\) will increase. Thus, increasing the number of common paths between \(E\) and \(D\) results in more information likely to be leaked towards \(E\) and a higher amount of distortion noise due to imperfection injected into \(N_C\). Therefore, unlike the perfect hardware case where the intercept probability is optimistically assumed to be only affected by the relationship between spatially resolvable paths of \(E\) and \(D\), we highlight that the level of hardware imperfections can significantly influence the secrecy performance.

The secrecy performance is evaluated from two perspectives. In Section 4, the primary design objective is to minimize the SOP. To do so, a closed form expression for the SOP is obtained and the OPA factor \(\tau_{opt}\) is derived through minimizing the SOP. In the second approach presented in Section 5, the OPA that maximizes the throughput \(\tau_{lo}\) subject to a maximum permissible SOP constraint is derived.

### 4 SOP ANALYSIS AND THE CORRESPONDING OPA STRATEGY

With the on-off transmission strategy described in Section 2, the SOP is expressed as \(\mathcal{P}_{SO} \triangleq \mathbb{P}_r\{C_D - C_E < R|G \in \xi\}\) for a fixed rate \(R\) based on a common codebook at \(S\) and \(D\). Utilizing on-off transmission, the source stops transmissions unless the instantaneous destination's channel gain \(G\) exceeds the threshold \(\mu\) which is determined relying on the conditions of the transmission region \(\xi\). Thus, to guarantee a positive \(R\) against the eavesdropper the minimum value for the power allocation factor is determined according to the transmission region described in dynamic on-off transmission, where, \(C_D = \log_2(1 + Y_{D,AN}) > R\). Therefore, using (6) we can conclude that

\[
Y_{D,AN} = \frac{\tau d}{\tau e + 1} > (T - 1) \implies \tau > \tau_{\text{min}} \triangleq \frac{T}{d - \epsilon T}, \tag{10}
\]

where \(T \triangleq T - 1\) with \(T \triangleq 2^b\) and therefore the overall channel gain threshold is \(G > \mu = \frac{(T - 1)(\tau e + 1)N_{\text{SNDR}}}{PM\alpha_d}\). On the other hand, based on \(Y_{D,AN}\) in (6), the SOP is given by

\[
\mathcal{P}_{SO} = \mathbb{P}_r \left\{ Y_{E,AN} > \frac{Y_{D,AN} - \overline{T}}{T} \right\} = \mathbb{P}_r \left\{ Y_{E,AN} > \frac{\tau d - \overline{T}(\tau e + 1)}{T(\tau e + 1)} \right\}, \tag{11}
\]

In order to examine (11), we derive the cumulative distribution function (CDF) of \(Y_{E,AN}\) given by

\[
F_{Y_{E,AN}}(x) \triangleq \mathbb{P}_r \left\{ \frac{\tau au}{1 - \tau} < x \right\} = \mathbb{P}_r \left\{ u < \frac{\lambda - (1 - \tau) R_E V + \tau cu + 1}{\tau (a - cx)} \right\}, \tag{12}
\]

and exploit the following helpful lemma.

**Lemma 1.** The CDF of r.v. \(\hat{\Lambda} \triangleq \frac{a_1 \Lambda}{a_1 \Lambda + a_3}\), where \(\Lambda\) is a nonnegative r.v. and \(a_i > 0\) represent positive constants, is obtained as
From the definition of CDF we have

\[
F_A(x) = \mathbb{P}_T \left\{ \frac{a_1 T}{a_2 T + a_3} \leq x \right\} = \mathbb{P}_T \{ (a_1 - a_2 x) \leq a_3 x \}. \tag{14}
\]

Proof. From the definition of CDF we have

\[
F_A(x) = \mathbb{P}_T \left\{ \frac{a_1 T}{a_2 T + a_3} \leq x \right\} = \mathbb{P}_T \{ (a_1 - a_2 x) \leq a_3 x \}. \tag{14}
\]

If \((a_1 - a_2 x) < 0\), the probability of (14) becomes one, while in the case of having \((a_1 - a_2 x) \geq 0\), it will be equal to

\[
F_A \left( \frac{a_1 x}{a_2 x + a_3} \right).
\]

Using Lemma, \(F_{I\Lambda}(x)\) is derived as

\[
F_{I\Lambda}(x) = \begin{cases} 
F_u \left( \frac{x((1-\tau) b + 1)}{\tau (a - cx)} \right) & ; 0 \leq x < \frac{1}{k_c}, \\
1 & ; x \geq \frac{1}{k_c},
\end{cases}
\]

where \(F_u \left( \frac{x((1-\tau) b + 1)}{\tau (a - cx)} \right)\) is acquired as

\[
F_u \left( \frac{x((1-\tau) b + 1)}{\tau (a - cx)} \right) = 1 - \mathbb{E}_\nu \left[ e^{\frac{-x}{\nu}} \right] = 1 - e^{-\frac{x}{\nu}} \int_0^\infty \frac{\nu^{N_{\nu} - 1}}{\Gamma(N_{\nu} - 1)} e^{-\left(\frac{1 + x}{\nu}\right)} d\nu = 1 - e^{-\frac{x}{\nu}} \left[ 1 + \frac{(1-\tau) b x}{\tau (a - cx)} \right]^{-N_{\nu} - 1} \tag{16}
\]

Now, given (11) the SOP is given by

\[
\mathcal{S}_SO = \begin{cases} 
\mathcal{S}_SO ^\circ (\tau) & ; \gamma_1(\tau) < T < \gamma_2(\tau) \\
0 & ; T \leq \gamma_1(\tau)
\end{cases}
\]

where \(\gamma_1(\tau) \triangleq \frac{\tau d_k + k_1}{\tau d_{k_2} + k_2} + 1\) and \(\gamma_2(\tau) \triangleq \frac{\tau d_k + k_1}{\tau d_{k_2} + k_2} + 1\) with \(k_1 \triangleq k_1 + k_2 + k_3, k_2 \triangleq k_2 + k_3, k_3 \triangleq k_3 + 1 \) and \(\mathcal{S}_SO ^\circ\) is given by

\[
\mathcal{S}_SO ^\circ (\tau) \triangleq \exp \left( -\frac{\tau d - (\nu + 1) \bar{T}}{\nu((\nu + 1) T - \nu + 1)} \right) \times \left[ 1 + \frac{(1-\tau) b (\tau d - (\nu + 1) \bar{T})}{(\nu + 1) T - \nu + 1} \right]^{-N_{\nu} - 1} \tag{18}
\]

Our new expression in (18) generalizes the SOP expression derived for the ideal hardware case in Reference 18 It should be remarked that, since we use on-off transmission scheme with regard to the fact that \(0 \leq \tau < 1\) we have to consider two further cases for the SOP. Therefore, the cases of \(T > \gamma_3\) with \(\gamma_3 \triangleq \frac{k_1}{k_2} + 1\) and \(< \frac{T}{\beta_0(1-k_3/E)}\) should be taken into account where \(S\) stops transmitting if one of these conditions holds true. From the practical point of view, the condition \(T > \gamma_3\) implies that unlike perfect hardware situation where the design parameter \(R_0\) is independent of transceivers hardware qualities, in our generalized considered case, \(R_0\) should be determined in accordance with the aggregate level of impairments imposed on the whole network, before the data transmission. Then, even if \(T < \gamma_3\), the source node examines the overall destination's channel feedback to determine if the constraint \(G < \frac{T}{\beta_0(1-k_3/E)}\) (or equivalently \(T > \frac{k_1}{1+dk_{tot}} = \gamma_2(1)\)) is satisfied and full power is assigned for AN transmission (ie, \(\tau = 0\)) or the source totally suspends its transmission.
Based on what was discussed above together with (17), finally the overall SOP is derived as

$$
\mathcal{P}^*_{SO} = \begin{cases} 
1 & T > \gamma_3 \\
\mathcal{P}^*_{SO}(\tau^*_{opt}) & T < \gamma_3 \text{ & } T < \gamma_2(1) \text{ & } \gamma_1(\tau^*_{opt}) < T < \gamma_2(\tau^*_{opt}) \\
0 & T < \gamma_3 \text{ & } T < \gamma_2(1) \text{ & } T < \gamma_1(\tau^*_{opt}) 
\end{cases}
$$

(19)

where the SOP is 1 for target secrecy rates above a threshold determined by the imperfection of the nodes, that is, $>\gamma_3$. When $T < \gamma_3$, the SOP approaches zero with increasing $P$. Our result is different from the ideal hardware scenario in which the SOP, regardless to any target secrecy rate, always approaches zero with increasing SNR.\(^{18,39}\)

Based on (19), $\mathcal{P}^*_{SO}(\tau^* )$ is attained by substituting the OPA factor $\tau^*_{opt}$ which minimizes the SOP in (17). From (19) it can be inferred that if the predefined target secrecy level satisfies $T < \gamma_3$, the OPA that minimizes the SOP can be derived. Minimizing the instantaneous SOP, with respect to the power allocation factor $\tau$ yields the optimum value $\tau^*_{opt}$ as follows

$$
\tau^*_{opt} = \arg \min_{\tau} \mathcal{P}^*_{SO}(\tau) \\
\text{s.t. } \tau_{min} < \tau < 1
$$

(20)

The minimization of $\mathcal{P}^*_{SO}(\tau)$ is equivalent to minimizing $\mathcal{P}^*_{SO}(\tau)$. However, because of the complicated mathematical structure of $\mathcal{P}^*_{SO}(\tau)$, it is non-trivial to simply investigate the monotonicity of $\mathcal{P}^*_{SO}(\tau)$. As an alternative solution, since we have $\mathcal{P}^*_{SO}(\tau) = \prod_{r} \left[ \log_2 \left( \frac{1+\beta \gamma_3(\tau)}{1+\beta \gamma_3(\tau)} \right) < R_3 | G \in \mathcal{E} \right]$ and also given that $\log(\cdot)$ is a monotonically increasing function, the minimization of $\mathcal{P}^*_{SO}$ is equivalent to the maximization of $\phi(\tau) \triangleq \frac{1+\beta \gamma_3(\tau)}{1+\beta \gamma_3(\tau)}$ as follows

$$
\tau^*_{opt} = \arg \max_{\tau} \phi(\tau) \\
\text{s.t. } \tau_{min} < \tau < 1
$$

(21)

Substituting $Y_{D,\text{AN}}$ and $Y_{E,\text{AN}}$, which was earlier obtained respectively in (6) and (7), $\phi(\tau)$ can be reformulated as

$$
\phi(\tau) \triangleq \frac{c_1 \tau^2 + c_2 \tau + c_3}{c_4 \tau^2 + c_5 \tau + c_6}
$$

(22)

where $c_1 \triangleq (e+d)(cu-bv)$, $c_2 \triangleq (e+d)(bv+1) + cu - bv$, $c_3 \triangleq bv+1 = c_6$, $c_4 \triangleq e(cu+au-bv)$ and $c_5 \triangleq e(bv+1) + cu + au - bv$. To obtain optimal points of $\phi(\tau)$ over $\tau$, we first investigate the convexity of $\phi(\tau)$. To do so, the first derivative of $\phi(\tau)$ with respect to $\tau$ is given by

$$
\frac{\partial \phi(\tau)}{\partial \tau} = \frac{\varepsilon_1 \tau^2 + \varepsilon_2 \tau + \varepsilon_3}{(c_4 \tau^2 + c_5 \tau + c_6)^2},
$$

(23)

where $\varepsilon_1 \triangleq c_1 c_5 - c_2 c_4$, $\varepsilon_2 \triangleq 2c_3(c_1 - c_4)$ and $\varepsilon_3 \triangleq c_3(c_2 - c_5)$. Since the denominator is always positive, we can readily find that the sign of $\frac{\partial \phi(\tau)}{\partial \tau}$ follows that of the numerator $\Omega(\tau) \triangleq \varepsilon_1 \tau^2 + \varepsilon_2 \tau + \varepsilon_3$. In other words, examining the sign of $\Omega(\tau)$ is sufficient to investigate the monotonicity of $\phi(\tau)$. Now, relying on corollary 1 in Reference 14 together with the sign of $\Omega(\tau)$ at the boundaries $\tau = \tau_{min}$ and $\tau = 1$, the following proposition is presented to solve the maximization of $\phi(\tau)$ in (21).

**Proposition 1.** Based on the sign of $\Omega(\tau)$ at the boundaries $\tau = \tau_{min}$ and $\tau = 1$, $\phi(\tau)$ may be convex, concave or it is possible to be neither convex nor concave in the feasible set $\tau \in (\tau_{min}, 1]$. Following this fact, the optimal point is given by

$$
\tau^*_{opt} = \begin{cases} 
\mathcal{F} \{ \max \{ \Omega(\tau_{min}), \Omega(\tau^*_{opt}), \Omega(\tau^*_1), \Omega(1) \} \} ; \Omega(\tau_{min}) > 0 \\
\mathcal{F} \{ \max \{ \Omega(\tau_{min}), \Omega(1) \} \} ; \Omega(\tau_{min}) < 0 \text{ & } \Omega(1) > 0 \\
\tau^*_1 ; \Omega(\tau_{min}) > 0 \text{ & } \Omega(1) < 0
\end{cases}
$$

(24)
where $\tau_1^* = (-\epsilon_2 + \sqrt{\epsilon_2^2 - 4\epsilon_1\epsilon_3})/(2\epsilon_1)$ and $\tau_2^* = (-\epsilon_2 - \sqrt{\epsilon_2^2 - 4\epsilon_1\epsilon_3})/(2\epsilon_1)$ are the zero-crossing points of $\Omega(\tau)$. The operator $\mathcal{T}(f(x))$ is defined as a function which extracts the point $x_i$ corresponding to $y_i \triangleq f(x_i)$. Please refer to Appendix A for the proof.

5 | SECRECY THROUGHPUT ANALYSIS AND CORRESPONDING OPA STRATEGY

In the previous section, we assume that the code rates are fixed and do not vary with $G$. In this section, a different approach is considered where the power allocation factor $\tau$ is optimized for different code rates, that is, the transmission code rate $R_t$ and source code rate $R_s$ are adapted for each channel realization of $D$. This leads to a higher throughput compared to the previous scheme at the expense of higher complexity. Hence, in this second approach the code rates $R_t$ and $R_s$ are potentially functions of $G$, that is, $R_t(G)$ and $R_s(G)$. Based on on-off transmission scheme, when $G \in G$, the average secrecy throughput is defined as $Y \triangleq E_G \{R_s(G)\}$ while in the case of $G \notin G$ we have $R_s(G) = 0$. Our aim is to maximize the throughput under a maximum tolerable SOP constraint. To do so, the maximization of $Y$, which is equivalent to the maximization of $R_s(G)$ for each destination’s channel realization, is accomplished over the parameters $R_t$ and power allocation factor $\tau$ to satisfy the requirement on the SOP, that is, $\mathcal{P}_{SO}(G) < \epsilon$. The throughput optimization problem is formulated as

$$
\tau_0^* = \arg \max_{\tau \in \mathcal{R}} R_s(G) \\
\text{s.t. } 0 < R_t(G) < R_s(G) \leq C_D \\
\mathcal{P}_{SO}(G) \leq \epsilon \\
0 \leq \tau \leq 1
$$

where the first constraint guarantees to have a reliable link to the intended receiver that is, corresponding transmission region of the second OPA strategy. The second condition imposes secrecy constraint in which the parameter $0 \leq \epsilon \leq 1$ is a predefined threshold that indicates the maximum tolerable SOP. The third condition is the power allocation constraint. By relaxing the optimization problem (25), it can be rewritten as follows, whereas the derivation is relegated to Appendix B.

$$
\tau_0^* = \arg \max_{\tau \in \mathcal{R}} R_s(\tau) \\
\text{s.t. } -\frac{d}{\tau e + 1} \geq k(\tau), \quad 0 < \tau < 1
$$

where $k(\tau) \triangleq \frac{R_s^{-1}(1-e)}{\tau}$ and $R_s(\tau)$ is given by

$$
R_s(\tau) \triangleq \log_2 \left( \frac{1 + Y_{DAN}}{1 + \tau k(\tau)} \right) = \log_2 \left( \frac{\tau(d + e) + 1}{\tau^2 \epsilon k(\tau) + \tau k(\tau) + \epsilon} \right) + 1. \tag{27}
$$

Notably, the transmission region constraint $\xi_{so} = \left\{ G | \frac{d}{\tau e + 1} \geq k(\tau) \right\}$ in (26) implies that $S$ only transmits when this condition is satisfied.

To solve the maximization problem in (26), we have to first investigate the behavior of $k(\tau)$. Using (16) and the definition of $k(\tau)$, the equation $F_{Y_{DAN}}(\tau k(\tau)) = 1 - \epsilon$ can be reformulated as follows

$$
Q(k) \triangleq \exp \left( -\frac{k(\tau)}{a - \epsilon \tau k(\tau)} \left[ 1 + \frac{(1 - \tau)k(\tau)}{a - \epsilon \tau k(\tau)} \right]^{-N_{e-C}} - \epsilon \right) \tag{28}
$$

where $k(\tau)$ is a monotonically increasing function in the feasible set $0 \leq \tau \leq 1$. (See Appendix C for the proof). From (28) the maximum value of $k(\tau)$, denoted by $k_{\max}$, is attained when $\tau = 1$ as

$$
k_{\max} = k(1) = -a ln(\epsilon)/(1 + c ln(\epsilon)) \tag{29}
$$
where \( Q(k) \) is a monotonically decreasing function of \( k \) (please refer to Appendix D for the proof). Thus, \( Q(k = 0) = Q_{\text{max}} = 1 - \epsilon \geq 0 \). Also, \( Q_{\text{min}} \) is acquired as

\[
Q_{\text{min}} = Q(k_{\text{max}}) = e^{\ln(\epsilon)} \left[ 1 - (1 - \tau) \frac{\ln(\epsilon)}{1 + (1 + \tau) \ln(\epsilon)} \right]^{-\frac{(N_eC)}{N_eC}} - \epsilon
\]  

(30)

In the above equation, \( e^{\ln(\epsilon)} \leq e^{\ln(\epsilon)} = \epsilon \). Thus, \( Q_{\text{min}} \leq \epsilon \left( 1 - (1 - \tau) \frac{\ln(\epsilon)}{1 + (1 + \tau) \ln(\epsilon)} \right)^{-\frac{(N_eC)}{N_eC}} - \epsilon \leq 0 \). We can easily conclude that \( Q(k) \) has a unique zero crossing point. Applying the bisection method we can find a value \( k \) which is the zero crossing point of \( Q(k) \) within the range \([0, k_{\text{max}}]\) for a given \( \tau \). To start bisection method, upper and lower bound of \( k \) are considered as \([k_l, k_u] = [0, k_{\text{max}}]\). To solve (26), optimal value of \( \tau \) should be found such that \( R_s \) is maximized. The optimal value of \( \tau \) is derived for two cases of \( R_s(1) \).

**Case 1.** \( R_s(\tau) \) is a concave function of \( \tau \). In this case, the optimal value is given by

\[
\tau_{s_{\text{opt}}}^* = \begin{cases} 
1, & Z > 0 \\
\tau^*, & \text{otherwise}
\end{cases}
\]

(31)

where \( \tau^* \) is the unique root of the following equation

\[
\frac{dR_s}{d\tau} = \frac{1}{\ln 2} \left( \frac{1}{(\tau e + 1)(\tau e + d)} - \frac{k + \tau \frac{dk}{d\tau}}{1 + \tau k} \right) = 0
\]

and \( Z = \frac{1}{\ln 2} \left( \frac{d}{(\tau + 1)(\tau + 1)} + \frac{(N_eC + 1) a \ln(\epsilon)}{1 + (\tau - \epsilon) a \ln(\epsilon)} \right) \).

**Case 2.** \( R_s(\tau) \) is a non-concave function of \( \tau \). In this case, the optimal value is given by

\[
\tau_{s_{\text{opt}}}^* = \begin{cases} 
\tau_1, & R_s(\tau_1) > R_s(1) \\
1, & R_s(\tau_1) < R_s(1) \}
\end{cases}
\]

(32)

\[
\begin{cases} 
\tau_2, & R_s(\tau_2') > R_s(\tau_2) \\
\tau_3, & R_s(\tau_3') < R_s(\tau_3) \}
\end{cases}
\]

(33)

where, \( \tau_1, \tau_2, \), and \( \tau_3 \) are discussed in Appendix E. Therefore, \( \tau_{s_{\text{opt}}}^* \) could be obtained using bisection method. As such, \( S \) only transmits when \( G \notin \xi_{s_{\text{opt}}} \). Otherwise, \( S \) keeps silent to guarantee a positive \( R_s \) and the only power allocation factor which could meet the transmission condition is the OPA that maximizes \( R_s(G) \). Therefore, the maximum secrecy throughput is defined as

\[
Y = \iint_{\xi_{s_{\text{opt}}}} R_{\text{opt}}(G)f_{G,G}(x,y)dxdy
\]

(34)

where \( R_{\text{opt}}(G) \) is the maximized secrecy rate for \( \tau_{s_{\text{opt}}}^* \) and \( f_{G,G}(x,y) \) is the joint probability density function (pdf) of \( G \) and \( G \). Since \( \xi_P \) and \( \xi_C \) have no common path, \( f_{G,G}(x,y) \) could be replaced by \( f_G(x) \times f_G(y) \). Similar to what is mentioned for \( v \) in Section 3, \( G \sim \text{Gamma}(N_C, 1) \) and \( G \sim \text{Gamma}(N_{D-C}, 1) \). Therefore, (34) can be rewritten as

\[
Y = \iint_{\xi_{s_{\text{opt}}}} R_{\text{opt}}(G)f_G(x)f_G(y)dxdy
\]

(35)

where \( f_G(x) = e^{-x/N_{D-C}} \) and \( f_G(y) = e^{-y/N_{C}} \). The secrecy throughput for MRT beamforming can be derived as a special case with \( \tau = 1 \) and \( k = k_{\text{max}} \) given in (29). Thus, \( R_{\text{opt}}(G) \) with MRT beamforming is derived as

\[
R_{\text{opt}}(G) = \log_2 \left( \frac{1 + \frac{d}{c+1}}{1 - \frac{dl}{c+1} \kappa} \right)
\]

(36)
Reddefining \( a = \frac{\hat{G}}{G + \hat{G}} \), \( c = \frac{\hat{G}}{G + \hat{G}} \), \( d = \frac{\hat{G}}{G + \hat{G}} \), and \( e = \hat{G}(G + \hat{G}) \), the secrecy rate in (36) can be re-expressed as

\[
R_{\text{secrecy}}(G) = \log_2 \left( \frac{(G + \hat{G})(1 + \hat{c} \ln e)((\hat{e} + \hat{d})(G + \hat{G}) + 1)}{(\hat{c}(G + \hat{G}) + 1)(G + \hat{G}(1 + (\hat{c} - \hat{a})\ln e))} \right) \tag{37}
\]

The transmission region for this case is \( \{ G|\hat{G} > \beta \} \), where \( \beta \) is

\[
\frac{1}{2\hat{d}} \left( -(2\hat{G}\hat{d} + \hat{G}\hat{c} \ln e + \hat{c}\hat{d} \ln e) + \sqrt{\hat{G} \ln e(\hat{c}\hat{d} \ln e) + 2\hat{G} \ln e(\hat{c}^2 \ln e - 4\hat{a}\hat{d} + \hat{G} \ln e \hat{c}^2 \hat{d}^2)} \right) \tag{38}
\]

Please refer to Appendix F for the proof.

Accordingly, the maximum secrecy throughput for MRT plan is derived as

\[
Y = \int_{0}^{\infty} \int_{0}^{\infty} \frac{e^{-y \gamma_{0,c} - 1} e^{-y \gamma_{N_c} - 1}}{(N_{D, c} - 1)! (N_{C} - 1)!} \log_2 \left( \frac{(x + y(1 + \hat{c} \ln e))(\hat{e} + \hat{d})(x + y + 1)}{(\hat{c}(x + y) + 1)(x + y(1 + (\hat{c} - \hat{a})\ln e))} \right) dxdy \tag{39}
\]

According to [40, 4.337.5], the above integral becomes as

\[
Y = \sum_{m=0}^{N_0 - N_C - 1} \frac{1}{(N_{D, c} - m - 1)!} \int_{0}^{\infty} f(y)e^{-y \gamma_{0,c} - 1} \beta^{N_0 - N_C - m - 1} [F(q_1) + F(q_2) - F(q_3) - F(q_4) + q_5]dy \tag{40}
\]

where \( F(q) = \frac{1}{\ln 2} \sum_{m=0}^{m} \frac{1}{(m-\mu)!} \left[ \left( -1 \right)^{p-\mu} q^{\mu-p} e^{-1} E_{1} \left[ -1 \right] q^{\mu-n} \right] + \sum_{n=0}^{m-\mu} \left( n-1 \right) m^{n-\mu-n} \right), \quad q_1 = \frac{1}{\beta+y(1+\hat{c}\ln e)}, \quad q_2 = \frac{e+\hat{d}}{(\hat{e}+\hat{d})(\beta+y+1)}, \quad q_3 = \frac{1}{\beta+y(1+\hat{c}\ln e)}, \quad q_4 = \frac{e}{\hat{d}(\beta+y)} \quad \text{and} \quad q_5 = \log_2 \frac{[\beta+y(1+\hat{c}\ln e)][\hat{e}+\hat{d}(\beta+y+1)]}{[\beta+y(1+\hat{c}\ln e)][\hat{e}+\hat{d}(\beta+y+1)]}. \)

Please refer to Appendix G for the proof.

To obtain a deeper insight, we proceed to investigate the secrecy throughput in High-SNR Regime. To do so, we consider the ideal hardware SNR in (8) and the definition of \( R_c(\tau) \) in (27). As such, the secrecy rate is derived as

\[
R_{\text{secrecy}} = \log_2 \left( \frac{1 + \kappa^{\infty}(\tau)}{1 + \tau k^{\infty}(\tau)} \right) \tag{41}
\]

where \( \kappa = Y_{D,AN}^{\infty} = \frac{1}{\eta_{\text{sec}}} \). Since \( R_{\text{secrecy}}(\tau) > 0 \), the upper bound of \( k^{\infty}(\tau) \) is acquired as \( k^{\infty}_{\text{max}} = \frac{\kappa}{\tau} \). Using (9) and (12) we can conclude that

\[
F_{Y_{E,AN}(x)}(x) \triangleq Pr \left\{ \frac{\tau au}{(1 - \tau)bv + \tau cu} < x \right\} = Pr \left\{ u < \left( \frac{(1 - \tau)bux}{\tau(a - cx)} \right) \right\} \tag{42}
\]

Using a similar process to (28), \( Q^{\infty}(k^{\infty}) \) is derived as

\[
Q^{\infty}(k^{\infty}) = \left[ 1 + \frac{(1 - \tau)k^{\infty}(\tau)}{a - \tau c k^{\infty}(\tau)} \right]^{-N_{E,c} - \varepsilon} - \varepsilon \tag{43}
\]

where \( k^{\infty}(\tau) \) is a monotonically increasing function in the feasible set \( 0 \leq \tau \leq 1 \), (Appendix H). Regarding (41) and its first derivative with respect to \( \tau \) which is equal to \( \frac{1}{\ln 2} \times \frac{d}{d\tau} \frac{k^{\infty}(\tau)}{1 + k^{\infty}(\tau)} < 0 \) and the monotonically increasing \( k^{\infty}(\tau) \) with respect to \( \tau \), we can conclude that \( R^{\infty}(\tau) \) is monotonically decreasing with \( \tau \). Thus, maximum secrecy rate at high-SNRs occurs for small \( \tau \). This result states that most of the power \( P \) should be allocated to AN signal while the remaining of the power is dedicated to the source for signal transmission. This is equivalent to the case where most of the power is allocated to AN in (18) where \( \tau \) is very close to zero. Therefore, in high-SNR regime it is not easily possible for the eavesdropper to intercept the transmitted signal and therefore signal transmission is performed in most secure state.
6 | NUMERICAL EXAMPLES

In this section, numerical illustrations are presented to verify the accuracy of the analytical results. The transmitter is considered to be a linear array with antenna spacing of half wavelength. The path loss is modeled as \( a(d_B) = a + b \cdot 10\log_{10}(d) \) according to experimental results in Reference 20 and the noise power is set to \( \sigma_n^2 = -50 \text{ dBm} \). In this model, \( d \) is the distance in meters, \( a \) and \( b \) were measured at the carrier frequency of 28 GHz as 61.4 and 2 respectively. For comparison of the systems with perfect \( (k = 0) \) and imperfect hardware and also to investigate the imperfection level effect on the secrecy performance, we have considered two values of EVM as \( k = 0.05 \) and \( k = 0.1 \) which lies within the range mentioned in [41, sect. 14.3.4] and also implemented in Reference 42 Transmitter is considered to be a uniform-linear-array with antenna spacing half wavelength and the destination is located at \( d_D = 100 \text{ m} \) from the source transmitter.

Figure 3 compares the SOP of MRT and AN beamforming for different hardware imperfection levels and different numbers of common paths \( N_C \). An eavesdropper is located at a distance \( d_E = 100 \text{ m} \) from the transmitter and \( M \) is set to 100. We can draw three conclusions based on what is observed in this figure. First, SOP is increased when \( N_C \) increases. The reason is that increasing the number of common paths, the eavesdropper will have more opportunities to intercept information from the received signal to the destination. Second, increasing the imperfection level brings about a higher SOP. This is because the imperfection has a higher impact on the received SNDR at the destination compared to the eavesdropper which results in a higher eavesdropping probability. Third, AN beamforming significantly outperforms MRT because AN provides effective interference at the eavesdropper which makes it more advantageous for security.

Figure 4 shows the SOP vs \( N_C \) for different amounts of secrecy rate. It is shown that as \( R_s \) increases, the difference between SOP of the perfect and imperfect hardware becomes larger. It is further noted that for \( R_s = 6 \text{ bits/s/Hz} \) the system with imperfect hardware is always in secrecy outage which causes the communication to be insecure. This agrees with our analytical results in (20) which explains that the system is in complete secrecy outage for the derived threshold.

In Figure 5, we plot the OPA \( r^*_{\text{opt}} \) for different hardware imperfection levels and transmit powers \( P \). The plot shows that \( r^*_{\text{opt}} \) decreases with higher imperfection levels resulting in more AN transmitted at the source. We also see that \( r^*_{\text{opt}} \) decreases with increasing \( P \), which means that more AN signals should be transmitted when the information signal is successfully decoded at the destination.

Figure 6 plots the secrecy throughput in terms of transmission power \( P \). It is reasonable that increasing the transmission power results in higher secrecy throughput. However, as previously mentioned, hardware imperfection reduces the SNDR at the destination more than the eavesdropper which results in a lower secrecy throughput compared with the ideal hardware case. For further comparison, we have included the baseline performance of equal power allocation between the useful signal and AN. The figure clearly shows that the OPA can achieve significantly higher secrecy throughput especially in the imperfect hardware scenario.

**FIGURE 3** SOP vs \( N_C \) for different levels of hardware imperfections \( (k_{tx} = k_{rx} = k) \) with \( M = 100, P = 5 \text{ dBm}, R_s = 5 \text{ bits/s/Hz}, N_D = 20, \text{ and } d_D = 100 \text{ m} \).
**FIGURE 4** SOP vs $N_C$ for different secrecy rates and hardware imperfection levels $k_{tx} = k_{rx} = 0.1$ with $P = 5$ dBm, $N_D = 20$, and $\Delta_D = 100$ m.

**FIGURE 5** OPA vs $P$ for different levels of hardware imperfections ($k_{tx} = k_{rx} = k$) with $M = 150$, $\Delta_D = 100$ m, $R_s = 5$ bits/s/Hz, and $N_D = 20$.

**FIGURE 6** Secrecy throughput in terms of $P$ for perfect and imperfect hardware, with $M = 100$, $\Delta_D = 100$ m, $N_D = 20$, $N_C = 16$, and $\epsilon = 0.01$. 
**Figure 7** Optimal power allocation factor that maximizes secrecy throughput in terms of $P$ for perfect and imperfect hardware with $M = 100$, $d_D = 100$ m, $N_D = 20$, and $\varepsilon = 0.01$

Figure 7 plots the OPA factor $\tau_{io}^*$ that maximizes the secrecy throughput for perfect and imperfect hardware cases. When the transmission power $P$ is very low, the power allocation factor is one because all the power should be dedicated to the information signal. By increasing $P$, the transmission link is guaranteed and therefore a reduction in $\tau_{io}^*$ means that the allocated power to AN increases to interfere with the eavesdropper. By comparing these two cases, we see that increasing hardware imperfection leads to a decrease in $\tau_{io}^*$ compared with ideal case. Thus, more power should be dedicated to AN to interfere with the eavesdropper and hence improve the secrecy performance of the system with imperfect hardware. In addition, when $P$ is high enough, we can observe that $\tau_{io}^*$ approaches zero as discussed in Section 5 for the high SNR regime.

7 | CONCLUSION

In high rate mm-wave communications systems, physical transceiver hardware imperfections can create a remarkable distortion in the emitted and received signals. This article examined the presence of hardware imperfections in mm-wave systems with multiple transmit antennas and slow-fading channels. The SOP and secrecy throughput is derived assuming on-off transmission and no knowledge of the eavesdropper CSI. Our results concluded that hardware imperfections and the number of common propagation paths can substantially decrease the secrecy performance. OPA solutions are derived to minimize the SOP and maximize the secrecy throughput. Simulation results highlight that the OPA factor varies according to the level of hardware imperfections which confirm the validity of our derived analytical results.

**ORCID**

Saeed Mashdour [https://orcid.org/0000-0001-9599-9870](https://orcid.org/0000-0001-9599-9870)

Majid Moradikia [https://orcid.org/0000-0001-9254-4811](https://orcid.org/0000-0001-9254-4811)

**REFERENCES**

1. Mukherjee A, Fakoorian SAA, Huang J, Swindlehurst AL. Principles of physical layer security in multiuser wireless networks: a survey. *IEEE Commun Surv Tutor*. 2014;16(3):1550-1573.
2. Chen X, Ng DWK, Gerstacker WH, Chen HH. A survey on multiple-antenna techniques for physical layer security. *IEEE Commun Surv Tutor*. 2017;19(2):1027-1053.
3. Yang N, Wang L, Geraci G, Elkashlan M, Yuan J, Di Renzo M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun Mag*. 2015;53(4):20-27.
4. Zhou X, Yan S, Hu J, Sun J, Li J, Shu F. Joint optimization of a UAV’s trajectory and transmit power for covert communications. *IEEE Trans Signal Process*. 2019;67(16):4276-4290.
5. Zhou X, Wu Q, Yan S, Shu F, Li J. UAV-enabled secure communications: joint trajectory and transmit power optimization. *IEEE Trans Veh Technol*. 2019;68(4):4069-4073.
6. Izanlou, M., Mohammadi, A. and Dosarajian-Moghadam, M., 2019. Optimal power allocation for physical layer security in device-to-device communications using untrusted relays. *Trans Emerg Telecommun Technol.*, 30(10), p.e3623.

7. Pandey, A. and Yadav, S., 2019. Physical-layer security for cellular multiuser two-way relaying networks with single and multiple decode-and-forward relays. *Trans Emerg Telecommun Technol.*, 30(12), p.e3639.

8. Rusek F, Persson D, Lau BK, et al. Scaling up MIMO: opportunities and challenges with very large arrays. *IEEE Signal Process Mag.* 2013;30(1):40-60.

9. Larsson EG, Edfors O, Tufvesson F, Marzetta TL. Massive MIMO for next generation wireless systems. *IEEE Commun Mag.* 2014;52(2):186-195.

10. Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. *IEEE Commun Mag.* 2015;53(6):21-27.

11. Goel S, Negi R. Guaranteeing secrecy using artificial noise. *IEEE Trans Wirel Commun.* 2008;7(6):2180-2189.

12. Zhou X, McKay MR. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. *IEEE Trans Veh Technol.* 2010;59(8):3831-3842.

13. Zarrabi H, Kuhestani A, Moradikia M. EE-RS and PA for untrusted relay network at high signal-to-noise ratio regime. *IET Commun.* 2016;10(16):2143-2148.

14. Kuhestani A, Mohammadi A, Wong KK, Yeoh PL, Moradikia M, Khandaker MR. Optimal power allocation by imperfect hardware analysis in untrusted relaying networks. *IEEE Trans Wirel Commun.* 2018;17:4302-4314.

15. Zhang X, Zhou X, McKay MR. On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels. *IEEE Trans Veh Technol.* 2013;62(5):2170-2181.

16. Xiong J, Wong KK, Ma D, Wei J. A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming. *IEEE Commun Lett.* 2012;16(9):1496-1499.

17. Moradikia M, Mashdour S, Jamshidi A. Joint optimal power allocation, cooperation beamforming, and Jammer selection design to secure untrusted relaying network. *Trans Emerg Telecommun Technol.* 2018;29(3):3276.

18. Ju Y, Wang HM, Zheng TX, Yin Q. Secure transmissions in millimeter wave systems. *IEEE Trans Commun.* 2017;65(5):2114-2127.

19. Ju Y, Wang HM, Zheng TX, Yin Q, Lee MH. Safeguarding millimeter wave communications against randomly located eavesdroppers. *IEEE Trans Wirel Commun.* 2018;17(4):2675-2689.

20. Akdeniz MR, Liu Y, Samimi MK, et al. Millimeter wave channel modeling and cellular capacity evaluation. *IEEE J Select Areas Commun.* 2014;32(6):1164-1179.

21. Ju Y, Wang HM, Zheng TX, Zhang Y, Yang Q, Yin Q. Secrecy throughput maximization for millimeter wave systems with artificial noise. Paper presented at: Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); September 2016:1–6; IEEE.

22. Ramadan YR, Minn H. Artificial noise aided hybrid precoding design for secure mmWave MISO systems with partial channel knowledge. *IEEE Signal Process Lett.* 2017;24(11):1729-1733.

23. Valliappan N, Lozano A, Heath RW. Antenna subset modulation for secure millimeter-wave wireless communication. *IEEE Trans Commun.* 2013;61(8):3231-3245.

24. Wang C, Wang HM. Physical layer security in millimeter wave cellular networks. *IEEE Trans Wirel Commun.* 2016;15(8):5569-5585.

25. Björnson E, Hoydis J, Kountouris M, Debbah M. Massive MIMO with non-ideal hardware: energy efficiency, estimation, and capacity limits. *IEEE Trans Info Theory.* 2014;60(11):7112-7139.

26. Schenk T. *RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation.* 61. 5. New York: Springer-Verlag; 2008.

27. Zhu J, Ng DWK, Wang N, Schober R, Bhargava VK. Analysis and design of secure massive MIMO systems in the presence of hardware impairments. *IEEE Trans Wirel Commun.* 2017;16(3):2001-2016.

28. Boulogeorgos AAA, Karas DS, Karagiannidis GK. How much does I/Q imbalance affect secrecy capacity? *IEEE Commun Lett.* 2016;20(7):1305-1308.

29. Moradikia M, Bastami H, Kuhestani A, Behroozi H, Hanzo L. Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments. *IEEE Access.* 2019;7:116942-116964.

30. Yang X, Matthaiou M, Yang J, Wen CK, Gao F, Jin S. Hardware-constrained millimeter-wave systems for 5G: challenges, opportunities, and solutions. *IEEE Commun Mag.* 2019;57(1):44-50.

31. Balakrishnan S, Wang P, Bhuyan A, Sun Z. On success probability of eavesdropping attack in 802.11 ad mmWave WLAN. Paper presented at: Proceedings of the 2018 IEEE International Conference on Communications (ICC); May 2018:1–6; IEEE.

32. Steinmetzer D, Chen J, Classen J, Knightly E, Hollick M. Eavesdropping with periscopes: experimental security analysis of highly directional millimeter waves. Paper presented at: Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS); September 2015:335–343; IEEE.

33. Studer C, Wenk M, Burg A. MIMO transmission with residual transmit-RF impairments. Paper presented at: Proceedings of the 2010 International ITG Workshop on Smart Antennas (WSA); February 2010:189–196; IEEE.

34. Hur S, Kim T, Love DJ, Krogmeier JV, Thomas TA, Ghosh A. Millimeter wave beamforming for wireless backhaul and access in small cell networks. *IEEE Trans Commun.* 2013;61(10):4391-4403.

35. Liu C, Li M, Hanly SV, Collings IB, Whiting P. Millimeter wave beam alignment: large deviations analysis and design insights. *IEEE J Select Areas Commun.* 2017;35(7):1619-1631.

36. Li M, Liu C, Hanly SV, Collings IB, Whiting P. Explore and eliminate: optimized two-stage search for millimeter-wave beam alignment. *IEEE Trans Wirel Commun.* 2019;18(9):4379-4393.
Along this line, by plugging the boundaries \( \tau = \tau_{\min} \) we expect for \( \tau = 1 \) into \( \Omega(\tau) \) we can find that the sign of both \( \Omega(1) \) and \( \Omega(\tau_{\min}) \) is unknown in the range of possible values of coefficients \( \epsilon_i \). Thus, the following conclusions can be drawn for \( \phi(\tau) \)

1. If \( \Omega(1), \Omega(\tau_{\min}) > 0 \), it is expected for \( \phi(\tau) \) to be neither convex nor concave as can be seen in Figure C1A,B. Moreover, both roots of \( \Omega(\tau) \) lie within the range of feasible set. So, in this situation the maximum of \( \phi(\tau) \) may happen at \( \tau = \tau_{\min} \) or \( \tau = 1 \) or possibly at \( \tau_1^*, \tau_2^* \in (0, 1) \) which denote the roots of \( \Omega(\tau) \) in the range of feasible set. The OPA factor \( \tau_{opt}^* \) is selected by comparing \( \Omega(\tau_{min}), \Omega(\tau_1^*), \Omega(\tau_2^*), \) and \( \Omega(1) \).

2. If \( \Omega(\tau_{min}) < 0, \Omega(1) > 0 \) we expect for \( \phi(\tau) \) to be a convex function as can be illustrated in Figure C1C. Here, the maximum of \( \phi(\tau) \) occurs at \( \tau = \tau_{min} \) or \( \tau = 1 \) and the OPA factor \( \tau_{opt}^* \) is chosen by comparing \( \Omega(\tau_{min}) \) and \( \Omega(1) \).

3. Finally if \( \Omega(\tau_{min}) > 0 \& \Omega(1) < 0 \). In this situation, as shown in Figure C1D, given that only \( \tau_{opt}^* = \tau_1^* \) lies within the feasible set and the other root is outside of this interval, the corollary 1 in Reference 14 holds true and it can be found that \( \phi(\tau) \) is a concave function in the feasible set.

### APPENDIX B

From the definition of \( \mathcal{P}_{SO} \) we have

\[
\mathcal{P}_{SO} \triangleq \mathbb{P}_r \{ C_E > R_t - R_s \} = \mathbb{P}_r \{ Y_{E,AN} > 2^{R_t-R_s} - 1 \} = 1 - F_{Y_{E,AN}}(2^{R_t-R_s} - 1),
\]  

(B1)

Using the constraint \( \mathcal{P}_{SO} \leq \epsilon \) and defining \( k(\tau) \triangleq \frac{F_{Y_{E,AN}}(1-\epsilon)}{\tau} \), we have

\[
R_s \leq R_t - \log_2(\tau k(\tau) + 1),
\]  

(B2)

Furthermore, since we have \( R_t \leq C_D \), the upper bound of \( R_s \) is acquired as

\[
R_s(\tau) \triangleq C_D - \log_2(\tau k(\tau) + 1) = \log_2\left( \frac{1 + Y_{D,AN}}{\tau k(\tau) + 1} \right),
\]  

(B3)
Having \( Y_{D,AN} \) in (6), we can reformulate (B3) given by
\[
R_s(G) \triangleq \log_2 \left( \frac{\tau(d + e) + 1}{\tau^2 e k(r) + \tau(k(r) + e) + 1} \right),
\]
(B4)

On the other hand to achieve positive secrecy rate, that is, \( R_s(G) \geq 0 \), the node S transmits signal when \( G \) satisfies the transmission region's constraint \( \chi_D, AN \geq \tau k \), resulting in transmission constraint as \( \frac{d}{\tau e + 1} \geq k(r) \).

**APPENDIX C**

The first order derivative of \( k(r) \) with respect to \( \tau \) is calculated as below using the derivation criterion for implicit functions
\[
\frac{dk}{d\tau} = -\frac{\partial Q}{\partial \tau} \cdot \frac{\partial Q}{\partial k} = -\frac{k^2 r_k^2 (a - c \tau k + (1 - \tau)k) + k N_{E-C}(k^2 r_k - 1)(a - c \tau k)}{(a - c \tau k + (1 - \tau)k) + N_{E-C}(a - c \tau k)(1 - \tau)},
\]
(C1)

Note that, \( N_{E-C}, r, k, k_{\text{max}}^2 \) are positive variables. In addition, to investigate the positivity/negativity of the term \( a - c \tau k \) appeared in both the numerator and denominator, we obtain its lower bound by inserting \( k_{\text{max}}^{\text{max}} = \frac{d}{\tau e + 1} \) therein as follows.
\[
a - c \tau k > a - c \tau k_{\text{max}}^{\text{max}} \Rightarrow a - c \tau k > a - c \tau k_{\text{max}}^{\text{max}} \cdot \frac{1 + k^2 (d + 1)}{\tau k_{\text{tot}}^2} > 0,
\]
(C2)

Thus the denominator is always positive, that is, \( A_2(k) > 0 \), and it can be easily found that the sign of \( \frac{dk}{d\tau} \) follows that of the term \( k^2 r_k - 1 \) in the numerator \( A_1(k) \). On the other hand, for practical values of \( a_D, a_E, \sigma_n^2 \), and \( k_{\text{tx}} \) we always have \( \frac{1}{k_{\text{tx}}} \gg k_{\text{max}}^{\text{max}} \) in the feasible set \( \tau \in [0, 1] \). Therefore, the case \( k > \frac{1}{k_{\text{tx}}} \) cannot occur in practice and the term \( k^2 r_k - 1 \) will be always negative. Based on abovementioned discussion, it is easy to examine that \( A_1(k) \) for practical values of different parameters therein is always negative, being responsible for the fact that \( k \) is monotonically increasing function of \( \tau \), that is, \( \frac{dk}{d\tau} > 0 \).

![Figure C1](image)

**Figure C1** Graphical representations of all possible cases of \( \phi(\tau) \) vs \( \tau \). Case I is illustrated in (A) and (B). Cases II and III have been respectively, illustrated in (C) and (D)

**APPENDIX D**

Since \( k \) is monotonically increasing by \( \tau \), \( k_{\text{max}}^{\text{max}} \) is obtained for \( \tau = 1 \). In addition, from (28) we know that, \( Q(k(\tau = 1)) = 0 \). Thus
\[
Q(k(\tau = 1)) = e^{-\frac{k(\tau)}{a - c \tau k}} [1 - \epsilon] = 0 \Rightarrow k_{\text{max}}^{\text{max}} = -\frac{a \ln \epsilon}{1 + c \ln \epsilon}
\]
(D1)
But, \( \frac{\partial Q}{\partial k} \) is

\[
\frac{\partial Q}{\partial k} = \frac{-a}{(a - crk)^2} e^{-\frac{k}{a - crk}} \left[ 1 + \frac{(1 - \tau)k}{a - crk} \right]^{-(N_{E-C})} - \left( N_{E-C} \right) e^{-\frac{k}{a - crk}} \left[ 1 + \frac{(1 - \tau)k}{a - crk} \right]^{-(N_{E-C}-1)} (1 - \tau) a
\]  \hspace{1cm} (D2)

From Appendix C, we know that \((a - crk) > 0\). Accordingly, using (D2) it is easily concluded that \( \frac{\partial Q}{\partial k} < 0 \).

**APPENDIX E**

Based on (27) and Proposition , we have

\[
R_{s_{\text{max}}} = \log_2 \left( \frac{1 + \Upsilon_0}{\tau k(\tau + 1)} \right).
\]

Thus, \( \frac{dR_s}{d\tau} = \frac{1}{\ln 2} \left( \frac{1}{(\tau e + (\tau + d)) + 1} - \frac{k + \tau \frac{dR_s}{d\tau}}{1 + \tau k} \right) \). But, \( \frac{d^2k}{d\tau^2} \) and in turn \( \frac{d^2R_s}{d\tau^2} \) are very convoluted terms and the convexity of \( k \) and \( R_s \) with respect to \( \tau \) is not straightforward to analyze mathematically. Thus, we proceed to consider the following cases. First, \( \frac{dR_s}{d\tau} = \frac{1}{\ln 2} (d - k) \) for \( \tau = 0 \). Since \( d_{\tau e + 1} \geq k(\tau) \), then \( d > k \) and hence \( \frac{dR_s}{d\tau} > 0, \tau = 0 \). Therefore, \( R_s \) is a nonconvex function of \( \tau \) in the interval \( 0 < \tau < 1 \). If \( \frac{d^2R_s}{d\tau^2} > 0 \), then \( R_s \) is a concave function of the \( \tau \). When \( \tau = 1 \), which is equivalent with \( k = k_{\text{max}} = -aln(\epsilon)/(1 + cln(\epsilon)) \), \( \frac{dR_s}{d\tau} \) is

\[
\frac{dR_s}{d\tau} = \frac{d}{(e + 1)(e + d + 1)} + \frac{(N_{E-C} + 1) a \ln e \left( 1 + \frac{c \ln e}{1 + c \ln e} \right)}{1 + (c - a) \ln e}, \tau = 1
\]  \hspace{1cm} (E1)

In this case in which \( R_s \) is a concave function of \( \tau \), if \( \frac{dR_s}{d\tau} > 0 \) for \( \tau = 1 \), then maximum of \( R_s \) will occur at \( \tau = 1 \). If \( \frac{dR_s}{d\tau} < 0 \) for \( \tau = 1 \), then \( R_s \) will have an extremum at the root of the equation \( \frac{dR_s}{d\tau} = 0 \). When \( R_s \) is non-concave, depending on sign of \( \frac{dR_s}{d\tau} \) at \( \tau = 1 \) and based on Figure E1, two possible cases are \( \frac{dR_s}{d\tau} > 0 \) and \( \frac{dR_s}{d\tau} < 0 \) for \( \tau = 1 \). Therefore, maximum amount of \( R_s(\tau) \) is

\[
\max R_s(\tau) = \begin{cases} 
\max(R_s(\tau_1), R_s(1)), & Z > 0 \\
\max(R_s(\tau_2'), R_s(\tau_3)), & \text{otherwise} 
\end{cases}
\]  \hspace{1cm} (E2)

Hence, \( \tau_{\text{opt}} \) could be derived as (33).

**FIGURE E1** Graphical representations of all possible cases of \( R_s(\tau) \) vs \( \tau \) when \( R_s(\tau) \) is non-concave. (A) represents case 1 in which \( \frac{dR_s}{d\tau} > 0 \) for \( \tau = 1 \). (B) case 2 in which \( \frac{dR_s}{d\tau} < 0 \) for \( \tau = 1 \)

**APPENDIX F**

\[
\xi_{to} = \left\{ \mathcal{G} \mid d \frac{\tau + 1}{e + 1} > k \right\} = \left\{ \mathcal{G} \mid \frac{\bar{d}(\hat{G} + \hat{C})}{\hat{e}(\hat{G} + \hat{C}) + 1} > k \right\}
\]  \hspace{1cm} (F1)
For MRT plan, \( \tau = 1 \) and \( k = k_{\text{max}} = -\text{aln}(\varepsilon)/(1 + \text{cln}(\varepsilon)) \). Therefore, \( \frac{\hat{d}(\hat{G} + \tilde{G})}{\hat{e}(\hat{G} + \tilde{G}) + 1} > k \) becomes as

\[
\frac{\hat{d}(\hat{G} + \tilde{G})}{\hat{e}(\hat{G} + \tilde{G}) + 1} > \frac{-\hat{a} \ln \varepsilon}{\hat{G} + \tilde{G} + \hat{c} \ln \varepsilon}
\]

(F2)

From (F2) we can conclude that

\[
\hat{G}^2 + \hat{G} \left( \hat{G} \left( 2 + \tilde{c} \ln \varepsilon + \frac{\hat{a} \ln \varepsilon}{\hat{d}} \right) + \hat{G}^2 \left( 1 + \tilde{c} \ln \varepsilon + \frac{\hat{a} \ln \varepsilon}{\hat{d}} \right) + \frac{\hat{a} \hat{G} \ln \varepsilon}{\hat{d}} \right) > 0
\]

(F3) is similar to \( x^2 + a_1 x + a_2 > 0 \) where \( x \) is substituted by \( \tilde{G} \), \( a_1 \) by \( \hat{G} \left( 2 + \tilde{c} \ln \varepsilon + \frac{\hat{a} \ln \varepsilon}{\hat{d}} \right) \) and \( a_2 \) by \( \hat{G}^2 \left( 1 + \tilde{c} \ln \varepsilon + \frac{\hat{a} \ln \varepsilon}{\hat{d}} \right) + \frac{\hat{a} \hat{G} \ln \varepsilon}{\hat{d}} \). Since \( \hat{G} \triangleq \| \hat{G}_0 \|^2 \) is positive, deriving the roots of the equation \( x^2 + a_1 x + a_2 \) for substituted \( x \), \( a_1 \) and \( a_2 \), we can conclude that (F3) holds for the case of (38).

**APPENDIX G**

Defining variable \( \bar{x} = x - \beta \), (39) becomes as

\[
\int_0^\infty \int_0^\infty e^{(\bar{x} + \beta) N_{D-C} - 1} \beta^{N_{D-C} - 1} m f_{G}(y) \left( \ln \left( 1 + \frac{1}{\beta + y(1 + \tilde{c} \ln \varepsilon)} \right) + \ln \left( 1 + \frac{\bar{x}}{\beta + y(1 + \tilde{c} \ln \varepsilon)} \right) \right) d\bar{x} d\ln \varepsilon
\]

(G1)

We can replace \( f_{G}(y) \) into the integrals by \( \frac{\beta^{N_{D-C} - 1}}{N_{D-C} - 1} \) to get

\[
\int_0^\infty \int_0^\infty e^{-Y} f_{G}(y) \left( \ln \left( 1 + \frac{1}{\beta + y(1 + \tilde{c} \ln \varepsilon)} \right) + \ln \left( 1 + \frac{\bar{x}}{\beta + y(1 + \tilde{c} \ln \varepsilon)} \right) \right) d\bar{x} d\ln \varepsilon
\]

(G2)

\[
Y = \frac{1}{\ln 2} \int_0^\infty \int_0^\infty e^{-Y} f_{G}(y) \left( \ln \left( 1 + \frac{1}{\beta + y(1 + \tilde{c} \ln \varepsilon)} \right) + \ln \left( 1 + \frac{\bar{x}}{\beta + y(1 + \tilde{c} \ln \varepsilon)} \right) \right) d\bar{x} d\ln \varepsilon
\]

(G3)

Using [40, 4.337.5], (G3) is changed to (40).
APPENDIX H

\[ \frac{dk^\infty}{d\tau} = -\frac{\partial Q^\infty}{\partial k^\infty} = -\frac{kbc^\infty \tau^2 - abk^\infty \tau^2}{ab\tau^2 - ab\tau^3} = \frac{abk^\infty - bck^\infty - ab^2}{ab - ab\tau} \tag{H1} \]

Since \(0 < \tau < 1\), denominator is positive. The numerator is equal to \(abk^\infty - bck^\infty = abk^\infty(1 - k^\infty k_{rs}^2)\) because \(c = k_{rs}^2 a\). Since \(a, b\) and \(k^\infty\) are positive, \(k^\infty\) is monotonically increasing by \(\tau\) when \(k^\infty < \frac{1}{k_{rs}^2} < k_{\text{max}}^\infty = \frac{\gamma}{\tau} \).