Optimal Power Allocation by Imperfect Hardware Analysis in Untrusted Relaying Networks

Ali Kuhestani, *Student Member, IEEE*, Abbas Mohammadi, *Senior Member, IEEE*, Kai-Kit Wong, *Fellow, IEEE*, Phee Lep Yeoh, *Member, IEEE*, Majid Moradikia, and Muhammad R. A. Khandaker, *Member, IEEE*

Abstract

By taking a variety of realistic hardware imperfections into consideration, we propose an optimal power allocation (OPA) strategy to maximize the instantaneous secrecy rate of a cooperative wireless network comprised of a source, a destination and an untrusted amplify-and-forward (AF) relay. We assume that either the source or the destination is equipped with a large-scale multiple antennas (LSMA) system, while the rest are equipped with a single antenna. To prevent the untrusted relay from intercepting the source message, the destination sends an intended jamming noise to the relay, which is referred to as destination-based cooperative jamming (DBCJ). Given this system model, novel closed-form expressions are presented in the high signal-to-noise ratio (SNR) regime for the ergodic secrecy rate (ESR) and the secrecy outage probability (SOP). We further improve the secrecy performance of the system by optimizing the associated hardware design. The results reveal that by beneficially distributing the tolerable hardware imperfections across the transmission and reception radio-frequency (RF) front ends of each node, the system's secrecy rate may be improved. The engineering insight is that equally sharing the total imperfections at the relay between the transmitter and the receiver provides the best secrecy performance. Numerical results illustrate that the proposed OPA together with the most appropriate hardware design significantly increases the secrecy rate.

A. Kuhestani and A. Mohammadi are with the Electrical Engineering Department, Amirkabir University of Technology, Tehran, Iran.

K.-K Wong and M. R. A. Khandaker are with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K.

P. L. Yeoh is with the School of Electrical and Information Engineering, The University of Sydney, NSW, Australia.

M. Moradikia is with the Electrical Engineering Department, Shiraz University of Technology, Shiraz, Iran.

Index Terms

Physical layer security, Untrusted relay, Hardware imperfections, Optimal power allocation, Hardware design

I. Introduction

Security in wireless communication networks is conventionally implemented above the physical layer using key based cryptography [1]. To complement these highly complex schemes, wireless transmitters can also be validated at the physical layer by exploiting the dynamic characteristics of the associated communication links [2], [3]. Physical layer security (PLS) is a promising paradigm for safeguarding fifth-generation (5G) wireless communication networks without incurring additional security overhead [3].

Massive multiple-input multiple-output (MIMO) systems as a key enabling technology of 5G wireless communication networks provide significant performance gains in terms of spectral efficiency and energy efficiency [4], [5]. This new technology employs coherent processing across arrays of hundreds or even thousands of base station (BS) antennas and supports tens or hundreds of mobile terminals [4]–[6]. As an additional advantage, massive MIMO is inherently more secure than traditional MIMO systems, as the large-scale antenna array exploited at the transmitter can precisely aim a narrow and directional information beam towards the intended receiver, such that the received signal-to-noise ratio (SNR) is several orders of magnitude higher than that at any incoherent passive eavesdropper [7]. However, these security benefits are severely hampered in cooperative networks where the intended receivers may also be potential eavesdroppers [8]–[10].

In the context of PLS, cooperative jamming which involves the transmission of additional jamming signals to degrade the received SNR at the potential eavesdropper can be applied by source [9], [10], the intended receiver node [8] or a set of nodes, i.e., source and destination or source and relay to beamform the jamming noise orthogonal to the spatial dimension of the desired signal [11], [12]. Recently, several works have considered the more interesting scenario of untrusted relaying [13]–[21] where the cooperative jamming is performed by the intended receiver, which is referred to as *destination-based cooperative jamming* (DBCJ).

In real life, an *untrusted*, i.e., honest-but-curious, relay may collaborate to provide a reliable communication. Several practical scenarios may include untrusted relay nodes, e.g., in ultra-dense heterogenous wireless networks where low-cost intermediate nodes may be used to assist the source-destination transmission. In these networks, it is important to protect the confidentiality

of information from the untrustworthy relay, while concurrently relying on it to increase the reliability of communication. Thanks to the DBCJ strategy [8], positive secrecy rate can still be attained in untrusted relay networks. In recent years, several works have focused on the performance analysis [13]–[16], power allocation [17]–[20] and security enhancement [18], [21] of untrusted relaying networks. To be specific, the authors in [17] proposed an optimal power allocation (OPA) strategy to maximize the instantaneous secrecy rate of one-way relaying network while two-way relaying scenario was considered in [18]. By exploiting the direct link, a source-based artificial noise injection scheme was proposed in [19] to hinder the untrusted relay from intercepting the confidential message. A power allocation strategy was also proposed in [19] to optimally determine the information and jamming signal powers transmitted by the source. In [20], the OPA problem with imperfect channel state information was investigated. Notably, all the aforementioned works considered perfect hardware in the communication network.

In practice, hardware equipments experience detrimental impacts of phase noise, I/Q imbalance, amplifier non-linearities, quantization errors, converters, mixers, filters and oscillators [22], [23]. Each of the imperfections distorts the signals in its own way. While hardware imperfections are unavoidable, the severity of the imperfections depends on the quality of the hardware used in the radio-frequency (RF) transceivers. The non-ideal behavior of each component can be modeled in detail for the purpose of designing compensation algorithms, but even after compensation there remain residual transceiver imperfections [23]. *This problem is more challenging especially in high rate systems such as LTE-Advanced and 5G networks exploiting inexpensive equipments* [22]. Although most contributions in security based wireless networks have assumed perfect transceiver hardware [8]–[21], or only investigated the impact of particular imperfections such as I/Q imbalance [25] or phase noise [26] in the presence of an external eavesdropper, this paper goes beyond these investigations by considering *residual hardware imperfections* in physical layer security design [22]–[24].

In this paper, we take into account the OPA in a two-hop amplify-and-forward (AF) untrusted relay network where all the nodes suffer from hardware imperfections and either the source or the destination is equipped with large-scale multiple antennas (LSMA) [27], [28] while the other nodes are equipped with a single antenna. The DBCJ protocol is operated in the first phase and then the destination perfectly removes the jamming signal via self interference cancelation in the second phase. For this system model, the main contributions of the paper are summarized as follows:

- Inspired by [22]–[24], we first present the generalized system model for transceiver hardware imperfections in our secure transmission network. Based on this, we calculate the received instantaneous signal-to-noise-plus-distortion-ratio (SNDR) at the relay and destination.
- We formulate the OPA between the source and destination that maximizes the instantaneous secrecy rate of untrusted relaying. Accordingly, novel closed-form solutions are derived for the exact OPA. In addition, new simple solutions are derived for the OPA in the high SNR regime.
- According to our OPA solutions, novel compact expressions are derived for the ergodic secrecy rate (ESR) and secrecy outage probability (SOP) in the high signal-to-noise-ratio (SNR) regime that can be applied to arbitrary channel fading distributions. To gain further insights, new closed-form expressions are presented over Rayleigh fading channels. The asymptotic results highlight the presence of a secrecy rate ceiling which is basically different from the prefect hardware case. We highlight that this ceiling phenomenon is independent of the fading characteristic of the two hops.
- We provide new insights for hardware design in DBCJ-based secure communications. To this end, under the cost constraint of transceiver hardware at each node, we formulate the hardware design problem for the aforementioned network to maximize the secrecy rate. The results reveal that the secrecy rate can be improved by optimally distributing the level of hardware imperfections between the transmit and receive RF front ends of each node.

Notation: We use bold lower case letters to denote vectors. $\mathbf{I}_N$ and $\mathbf{0}_{N\times 1}$ denote the Identity matrix and the zeros matrix, respectively. $\|.\|$, $(.)^H$ and $(.)^T$ denote the Euclidean norm, conjugate transpose and transpose operators, respectively; $\mathbb{E}_x\{\cdot\}$ stands for the expectation over the random variable (r.v.) x; $\Pr(\cdot)$ denotes the probability; $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (pdf) and cumulative distribution function (cdf) of the r.v. X, respectively; the $\mathcal{CN}(\mu,\sigma^2)$ denotes a circularly symmetric complex Gaussian RV with mean μ and variance σ^2; $\mathrm{diag}(\mathbf{A})$ stands for the main diagonal elements of matrix A; $\mathrm{Ei}(x)$ is the exponential integral [34, Eq. (8.211)]. $[\cdot]^+ = \max\{0, x\}$ and $\max$ stands for the maximum value.

II. Signal and System Representation

A. System Model

As shown in Fig. 1, the system model under consideration is a wireless network with one source (S), one destination (D) and one untrusted AF relay (R). While R is equipped with one

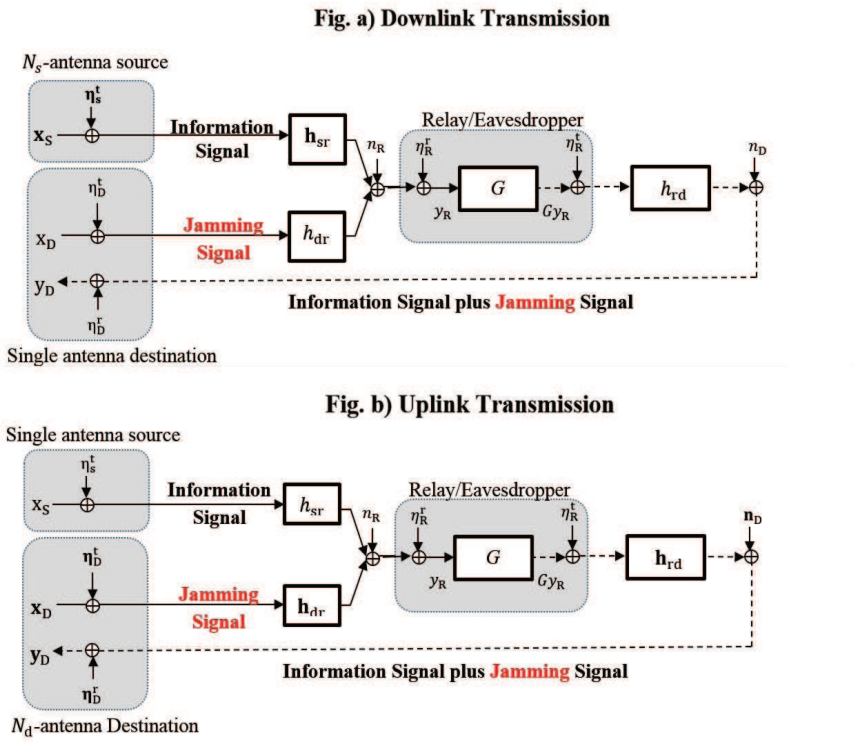

Fig. 1. Secure transmission under the presence of transceiver imperfections. The first and the second figures show the downlink and the uplink transmissions, respectively. The relay acts as both helper and eavesdropper. The solid lines represent the first phase of transmission while the dashed line represents the second phase of transmission.

antenna, S or D is equipped with LSMA denoted by $N_{\rm s}$ or $N_{\rm d}$, respectively [29], [30]. This corresponds to the downlink (DL) and uplink (UL) scenarios in a cellular system where the base station is equipped with a LSMA and the mobile user and relay are equipped with a single antenna [29]. In the DL scenario, S has many antennas, whereas D has a single antenna. The opposite applies to the UL scenario.

All the nodes operate in a half-duplex mode. Accordingly, D cannot receive the transmitted signal from S while transmitting the jamming signal and hence, the direct link between S and D is unavailable. We also assume that the channels satisfy the reciprocity theorem [8]. In DL transmission, the complex Gaussian channel from S to R and R to D are denoted by $\mathbf{h}_{\rm sr} \sim \mathcal{CN}(\mathbf{0}_{N_{\rm s}\times 1}, \mu_{\rm sr}\mathbf{I}_{N_{\rm s}})$ and $h_{\rm rd} \sim \mathcal{CN}(0, \mu_{\rm rd})$, respectively, and for UL transmission, they are denoted by $h_{\rm sr} \sim \mathcal{CN}(0, \mu_{\rm sr})$ and $\mathbf{h}_{\rm rd} \sim \mathcal{CN}(\mathbf{0}_{N_{\rm d}\times 1}, \mu_{\rm rd}\mathbf{I}_{N_{\rm d}})$, respectively. We consider slow fading such that the channel coefficients vary independently from one frame to another frame and, they do not change within one frame. The additive white noise n_i ($i \in \{\rm R, D\}$) at each receiver is represented by a zero-mean complex Gaussian variable with variance N_0. We define the SNRs per link as

$\gamma_{\rm sr}\overset{\Delta}{=}\rho\|\mathbf{h}_{\rm sr}\|^2$ and $\gamma_{\rm rd}\overset{\Delta}{=}\rho\|\mathbf{h}_{\rm rd}\|^2$ and hence, the average SNRs per branch is given by $\overline{\gamma}_{\rm sr}=\rho\mu_{\rm sr}$ and $\overline{\gamma}_{\rm rd}=\rho\mu_{\rm rd}$, where $\rho=\frac{P}{N_0}$ represents the transmit SNR of the network. The maximum ratio transmission (MRT) beamforming and maximal ratio combining (MRC) processing are applied at the multi-antenna node to improve the overall system performance [29]. Let $\nu=\frac{\gamma_{\rm sr}}{\gamma_{\rm rd}}$ represent the ratio between the source-to-relay and relay-to-destination SNRs. With LSMA, we consider $\nu\gg 1$ in the DL scenario while $\nu\ll 1$ in the UL scenario. These two special cases are taken into account in this paper. As observed in the numerical results, the analysis are satisfactory even for moderate values of ν.

The DBCJ technique is applied to degrade the received signal at the untrusted relay such that it cannot decipher the desired information. The whole transmission is performed based on a time-division multiple-access (TDMA) based protocol such that the message transmission is divided into two phases, i.e. the broadcast phase and the relaying phase. We consider a total transmit power budget for S and D of P with power allocation factor $\lambda\in(0,1)$ such that the transmit powers at S and D are λP and $(1-\lambda)P$, respectively [14], [18]. As such, during the first phase, while S transmits the intended signal with power λP, concurrently D jams with a Gaussian noise to confuse the untrusted relay with power $(1-\lambda)P$. For simplicity, the transmit power at R is set to P and accordingly, in the second phase of transmission, R simply broadcasts the amplified version of the received signal with power of P.

In order to consider the residual transceiver imperfections (after conventional compensation algorithms have been applied) at node i, $i\in\{\mathrm{S},\mathrm{R},\mathrm{D}\}$, the generalized system model from [22] is taken into account. The imperfection at transmission and reception segments denoted by $\eta_{\rm i}^t$ and $\eta_{\rm i}^r$ respectively, are introduced as distortion noises. The experimental results in [23] and many theoretical investigations in [23], [31] have verified that these distortion noises are well-modeled as Gaussian distributions due to the central limit theorem. A key property is that the variance of distortion noise at an antenna is proportional to the signal power at that antenna [23]. Accordingly, for the DL scenario, we have [23]

$$\begin{aligned}
&\boldsymbol{\eta}_{\rm S}^t\sim\mathcal{CN}\Big(0,\frac{\lambda P{k_{\rm S}^t}^2}{\|\mathbf{h}_{\rm sr}\|^2}\,\mathrm{diag}(|h_{\mathrm{sr}_1}|^2\ \ldots\ |h_{\mathrm{sr}_{N_{\rm s}}}|^2)\Big),\\
&\eta_{\rm D}^t\sim\mathcal{CN}\Big(0,(1-\lambda)P{k_{\rm D}^t}^2\Big),\\
&\eta_{\rm D}^r\sim\mathcal{CN}\Big(0,P{k_{\rm D}^r}^2|h_{\rm rd}|^2\Big).
\end{aligned}\tag{1}$$

Furthermore, we have

$$\begin{aligned}
&\eta_{\mathrm{S}}^{t} \sim \mathcal{CN}\Big(0, \lambda P k_{\mathrm{s}}^{t2}\Big),\\
&\boldsymbol{\eta}_{\mathrm{D}}^{t} \sim \mathcal{CN}\Big(0, \frac{(1-\lambda)P {k_{\mathrm{D}}^{t}}^{2}}{\|\mathbf{h}_{\mathrm{rd}}\|^2}\ \mathrm{diag}(|h_{\mathrm{rd}_1}|^2\ \ldots\ |h_{\mathrm{rd}_{N_{\mathrm{d}}}}|^2)\Big),\\
&\boldsymbol{\eta}_{\mathrm{D}}^{r} \sim \mathcal{CN}\Big(0, P {k_{\mathrm{D}}^{r}}^{2} \mathrm{diag}(|h_{\mathrm{rd}_1}|^2\ \ldots\ |h_{\mathrm{rd}_{N_{\mathrm{d}}}}|^2)\Big),
\end{aligned} \tag{2}$$

for the UL scenario. The imperfections at R of both cases are also given by

$$\begin{aligned}
&\eta_{\mathrm{R}}^{t} \sim \mathcal{CN}\Big(0, P {k_{\mathrm{R}}^{t}}^{2}\Big),\\
&\eta_{\mathrm{R}}^{r} \sim \mathcal{CN}\Big(0, P {k_{\mathrm{R}}^{r}}^{2}\Big[\lambda\|\mathbf{h}_{\mathrm{sr}}\|^2 + (1-\lambda)\|\mathbf{h}_{\mathrm{rd}}\|^2\Big]\Big),
\end{aligned} \tag{3}$$

where the design parameters k_i^t, $k_i^r > 0$ for $i \in \{\mathrm{S}, \mathrm{R}, \mathrm{D}\}$ characterize the level of imperfections in the transmitter and receiver hardware, respectively. These parameters can be interpreted as the error vector magnitudes (EVMs). EVM determines the quality of RF transceivers and is defined as the ratio of the average distortion magnitude to the average signal magnitude. Since the EVM measures the joint effect of different hardware imperfections and compensation algorithms, it can be measured directly in practice [22]. 3GPP LTE has EVM requirements in the range of $k_i^t, k_i^r \in [0.08, 0.175]$, where smaller values are needed to achieve higher spectral efficiencies [24].

Remark 1 (Co-channel Interference): The analysis in this paper supports the scenario of large enough number of interfering signals, which is typical in wireless environments where the Gaussian assumption for the interference is valid by applying the central limit theorem [32].

B. Signal Representation

Let us denote x_{S} and x_{D} as the unit power information signal and the jamming signal, respectively. According to the combined impact of hardware imperfections which is well-addressed by a generalized channel model [22], the received signal at R for DL and UL scenarios can be expressed, respectively as

$$y_{\mathrm{R}}^{\mathrm{DL}} = \Big(\sqrt{\lambda P}\mathbf{w}_{\mathrm{S}}^{T} x_{\mathrm{S}} + {\boldsymbol{\eta}_{\mathrm{S}}^{t}}^{T}\Big)\mathbf{h}_{\mathrm{sr}} + \Big(\sqrt{(1-\lambda)P}x_{\mathrm{D}} + {\boldsymbol{\eta}_{\mathrm{D}}^{t}}^{T}\Big)h_{\mathrm{rd}} + \eta_{\mathrm{R}}^{r} + n_{\mathrm{R}}, \tag{4}$$

and

$$y_{\mathrm{R}}^{\mathrm{UL}} = \Big(\sqrt{\lambda P}x_{\mathrm{S}} + {\eta_{\mathrm{S}}^{t}}^{T}\Big)h_{\mathrm{sr}} + \Big(\sqrt{(1-\lambda)P}\mathbf{w}_{\mathrm{D}}^{T} x_{\mathrm{D}} + {\boldsymbol{\eta}_{\mathrm{D}}^{t}}^{T}\Big)\mathbf{h}_{\mathrm{rd}} + \eta_{\mathrm{R}}^{r} + n_{\mathrm{R}}, \tag{5}$$

where $\mathbf{w}_{\mathrm{S}} = \frac{\mathbf{h}_{\mathrm{sr}}{}^{H}}{\|\mathbf{h}_{\mathrm{sr}}\|}$ and $\mathbf{w}_{\mathrm{D}} = \frac{\mathbf{h}_{\mathrm{rd}}{}^{H}}{\|\mathbf{h}_{\mathrm{rd}}\|}$ represent the MRT transmit weight vectors at S and D, respectively. Observe from (4) and (5) that the propagated distortion noises by S and D, and the self-distortion noise at R are treated as interference at the untusted relay which is a potential eavesdropper. As a result, the engineering insight is to beneficially forward these hardware imperfections to make the system secure instead of injecting more artificial noise by S [9], [10], [19], D [13]–[17], [20] or a friendly jammer [18].

Then the relay amplifies its received signal in the first phase by an amplification factor of [1]

$$G = \sqrt{\frac{P}{\mathbb{E}|y_{\mathrm{R}}|^2}} = \sqrt{\frac{\rho}{A_G\lambda + B_G}}, \tag{6}$$

where $A_G = (\gamma_{\mathrm{sr}} - \gamma_{\mathrm{rd}})(1 + {k_{\mathrm{R}}^r}^2) + {k_{\mathrm{S}}^t}^2\gamma_{\mathrm{u}} - {k_{\mathrm{D}}^t}^2\gamma_{\mathrm{v}}$ and $B_G = \gamma_{\mathrm{rd}}(1 + {k_{\mathrm{R}}^r}^2) + {k_{\mathrm{D}}^t}^2\gamma_{\mathrm{v}} + 1$. Note that in the DL scenario $\gamma_{\mathrm{u}} = \rho\sum|h_{\mathrm{sr}_i}|^4/\|\mathbf{h}_{\mathrm{sr}}\|^2$ and $\gamma_{\mathrm{v}} = \gamma_{\mathrm{rd}}$, and in the UL scenario $\gamma_{\mathrm{u}} = \gamma_{\mathrm{sr}}$ and $\gamma_{\mathrm{v}} = \rho\sum|h_{\mathrm{rd}_i}|^4/\|\mathbf{h}_{\mathrm{rd}}\|^2$. Then, the received signal at D for DL and UL scenarios after self-interference (or jamming signal) cancelation are respectively, given by

$$\mathbf{y}_{\mathrm{D}}^{\mathrm{DL}} = \underbrace{G\sqrt{\lambda P}\mathbf{w}_{\mathrm{S}}^{H}\mathbf{h}_{\mathrm{sr}}h_{\mathrm{rd}}x_{\mathrm{S}}}_{\text{Information signal}} + \underbrace{Gh_{\mathrm{rd}}n_{\mathrm{R}} + n_{\mathrm{D}}}_{\text{Noise}} + \underbrace{G{\boldsymbol{\eta}_{\mathrm{S}}^t}^{T}\mathbf{h}_{\mathrm{sr}}h_{\mathrm{rd}} + G\eta_{\mathrm{R}}^r h_{\mathrm{rd}} + G{\eta_{\mathrm{D}}^t}^{T}h_{\mathrm{rd}}h_{\mathrm{dr}} + \eta_{\mathrm{R}}^t h_{\mathrm{rd}} + \eta_{\mathrm{D}}^r}_{\text{Distortion noise}}, \tag{7}$$

and

$$\mathbf{y}_{\mathrm{D}}^{\mathrm{UL}} = \underbrace{G\sqrt{\lambda P}h_{\mathrm{sr}}\mathbf{h}_{\mathrm{rd}}x_{\mathrm{S}}}_{\text{Information signal}} + \underbrace{G\mathbf{h}_{\mathrm{rd}}n_{\mathrm{R}} + \mathbf{n}_{\mathrm{D}}}_{\text{Noise}} + \underbrace{G{\eta_{\mathrm{S}}^t}^{T}h_{\mathrm{sr}}\mathbf{h}_{\mathrm{rd}} + G\eta_{\mathrm{R}}^r\mathbf{h}_{\mathrm{rd}} + G{\boldsymbol{\eta}_{\mathrm{D}}^t}^{T}\mathbf{h}_{\mathrm{rd}}\mathbf{h}_{\mathrm{dr}} + \eta_{\mathrm{R}}^t\mathbf{h}_{\mathrm{rd}} + \boldsymbol{\eta}_{\mathrm{D}}^r}_{\text{Distortion noise}}. \tag{8}$$

According to (4) and (5) and after some algebraic manipulations, the SNDR at R is given by

$$\gamma_{\mathrm{R}} = \frac{\lambda\nu}{A_{\mathrm{R}}\lambda + B_{\mathrm{R}}}, \tag{9}$$

where $A_{\mathrm{R}} = {k_{\mathrm{R}}^r}^2\nu + {k_{\mathrm{S}}^t}^2\frac{\gamma_{\mathrm{u}}}{\gamma_{\mathrm{rd}}} - {k_{\mathrm{D}}^t}^2\frac{\gamma_{\mathrm{v}}}{\gamma_{\mathrm{rd}}} - {k_{\mathrm{R}}^r}^2 - 1$ and $B_{\mathrm{R}} = 1 + {k_{\mathrm{R}}^r}^2 + {k_{\mathrm{D}}^t}^2\frac{\gamma_{\mathrm{v}}}{\gamma_{\mathrm{rd}}} + \frac{1}{\gamma_{\mathrm{rd}}}$. Based on (7) and (8) and after some manipulations, the SNDR at D can be calculated as

$$\gamma_{\mathrm{D}} = \frac{\lambda\gamma_{\mathrm{sr}}}{A_{\mathrm{D}}\lambda + B_{\mathrm{D}}}, \tag{10}$$

where $A_{\mathrm{D}} = (\gamma_{\mathrm{sr}} - \gamma_{\mathrm{rd}})({k_{\mathrm{D}}^r}^2{k_{\mathrm{R}}^r}^2 + {k_{\mathrm{R}}^r}^2{k_{\mathrm{R}}^t}^2 + k_{\mathrm{R}}^2 + {k_{\mathrm{D}}^r}^2) + \gamma_{\mathrm{u}}({k_{\mathrm{D}}^r}^2{k_{\mathrm{S}}^t}^2 + {k_{\mathrm{R}}^t}^2{k_{\mathrm{S}}^t}^2 + {k_{\mathrm{S}}^t}^2) + \gamma_{\mathrm{v}}({k_{\mathrm{D}}^r}^2{k_{\mathrm{D}}^t}^2 -$

[1] In our analysis, we assume that the EVMs are perfectly known and will consider estimation errors in our future work.

${k_{\rm R}^t}^2{k_{\rm D}^t}^2-{k_{\rm D}^t}^2)+(\nu-1)(1+{k_{\rm R}^r}^2)+\frac{\gamma_{\rm u}}{\gamma_{\rm rd}}{k_{\rm S}^t}^2-\frac{\gamma_{\rm v}}{\gamma_{\rm rd}}{k_{\rm D}^t}^2$ and $B_{\rm D}=\gamma_{\rm rd}({k_{\rm R}^r}^2{k_{\rm D}^r}^2+{k_{\rm R}^r}^2{k_{\rm R}^t}^2+k_{\rm R}^2+{k_{\rm D}^r}^2)+\gamma_{\rm v}({k_{\rm D}^r}^2{k_{\rm D}^t}^2+{k_{\rm R}^t}^2{k_{\rm D}^t}^2+{k_{\rm D}^t}^2)+\frac{\gamma_{\rm v}}{\gamma_{\rm rd}}{k_{\rm D}^t}^2+\frac{1}{\gamma_{\rm rd}}+k_{\rm R}^2+{k_{\rm D}^r}^2+2$. We define $k_{\rm R}^2\triangleq{k_{\rm R}^t}^2+{k_{\rm R}^r}^2$ and $k_{\rm D}^2\triangleq{k_{\rm D}^t}^2+{k_{\rm D}^r}^2$ as the total imperfection level at R and D, respectively.

Remark 2 (Perfect Hardware): The received SNRs at R and D with perfect hardware were derived in [13], [14], [17]. When setting the level of imperfections at the nodes to zero, the derived SNDRs in this section reduce to the special case as follows [14]

$$\gamma_{\rm R}^{\rm perfect}=\frac{\lambda\gamma_{\rm sr}}{(1-\lambda)\gamma_{\rm rd}+1}\quad\text{and}\quad\gamma_{\rm D}^{\rm perfect}=\frac{\lambda\gamma_{\rm sr}\gamma_{\rm rd}}{\lambda\gamma_{\rm sr}+(2-\lambda)\gamma_{\rm rd}+1}. \tag{11}$$

As can be seen, the mathematical structure of the derived SNDRs in (9), (10) are more complicated compared to the perfect hardware case in (11), since the terms $\frac{\gamma_{\rm u}}{\gamma_{\rm rd}}$ and $\frac{\gamma_{\rm u}}{\gamma_{\rm rd}}$ manifest in the denominator. As such, it is non-trivial to propose an OPA solution for the general scenario of imperfect hardware. This generalization is done in Section III and is a main contribution of this work.

For DL scenario, (9) and (10) are simplified to

$$\gamma_{\rm R}=\frac{a_L\lambda}{\lambda+b_L}\quad\text{and}\quad\gamma_{\rm D}=\frac{c_L\lambda}{\lambda+d_L}, \tag{12}$$

where

$$a_L=\frac{1}{\xi_1-1},\quad b_L=\frac{\tau_1}{(\xi_1-1)\nu},\quad c_L=\frac{\gamma_{\rm rd}}{\tau_2\gamma_{\rm rd}+\xi_1}\quad\text{and}\quad d_L=\frac{\tau_3\gamma_{\rm rd}+\tau_4}{\nu(\tau_2\gamma_{\rm rd}+\xi_1)}, \tag{13}$$

and, $\tau_1=1+{k_{\rm R}^r}^2+{k_{\rm D}^t}^2$, $\tau_2={k_{\rm D}^r}^2{k_{\rm R}^r}^2+{k_{\rm R}^r}^2{k_{\rm R}^t}^2+k_{\rm R}^2+{k_{\rm D}^r}^2$, $\tau_3=\tau_2+{k_{\rm D}^t}^2{k_{\rm D}^r}^2+{k_{\rm R}^t}^2{k_{\rm D}^t}^2+{k_{\rm D}^t}^2$, $\tau_4=2+k_{\rm R}^2+k_{\rm D}^2$ and $\xi_1=1+{k_{\rm R}^r}^2$. Moreover, for UL scenario, we obtain

$$\gamma_{\rm R}=\frac{a_S\lambda}{1-\lambda}\quad\text{and}\quad\gamma_{\rm D}=\frac{b_S\lambda}{\lambda+c_S}, \tag{14}$$

where

$$a_S=\frac{\nu}{\xi_1},\quad b_S=\frac{\gamma_{\rm sr}}{(\gamma_{\rm sr}-\gamma_{\rm rd})\tau_2+(\nu-1)\xi_1}\quad\text{and}\quad c_S=\frac{\tau_2\gamma_{\rm rd}+\xi_2}{(\gamma_{\rm sr}-\gamma_{\rm rd})\tau_2+(\nu-1)\xi_1}, \tag{15}$$

and $\xi_2=2+k_{\rm R}^2+{k_{\rm D}^r}^2$. Based on (12) and (14), we can conclude that although the intercept probability is reduced by increasing the imperfection at R, the secrecy rate is also degraded. It is, therefore, of great interest to intelligently distribute the tolerable hardware imperfections across the transmission and reception radio frequency (RF) front ends of R (and other nodes) to improve the secrecy rate of the network. This hardware design approach is analyzed in Section

VI and is a main contribution of this paper.

III. Optimal Power Allocation

This section proceeds to analyze the optimal power allocation problem with the aim of maximizing the instantaneous secrecy rate. Extending the results in [17], [19], [20] where the OPA was solved for perfect hardware, we investigate the power allocation factor λ under the presence of hardware imperfections. To do so, the instantaneous secrecy rate is evaluated by [8]

$$R_s = \frac{1}{2\ln 2}\Big[\ln(1+\gamma_{\rm D}) - \ln(1+\gamma_{\rm R})\Big]^+. \tag{16}$$

By substituting $\lambda = 0$ into (9), (10) and then (16), we find $R_s = 0$. Since our goal is to distribute the power optimally between S and D, a non-negative secrecy rate is achievable. As such, the instantaneous secrecy rate can be reformulated as

$$R_s = \frac{1}{2\ln 2}\Big[\ln(1+\gamma_{\rm D}) - \ln(1+\gamma_{\rm R})\Big]. \tag{17}$$

Given that $\log(\cdot)$ is monotonically increasing, the maximization of R_s is equivalent to the maximization of

$$\phi(\lambda) \triangleq \frac{1+\gamma_{\rm D}}{1+\gamma_{\rm R}}. \tag{18}$$

Therefore, the OPA factor $\lambda^\star$ can be obtained by solving the following constrained optimization problem

$$\begin{aligned} \lambda^\star = \ & \arg \ \ \max \ \Big\{\phi(\lambda)\Big\} \\ & \text{s.t.} \qquad 0 < \lambda \leq 1 \end{aligned} \tag{19}$$

Lemma 1: $f(x)$ is a quasi-concave function in $\mathbb{R}$, if and only if [33, Section 3.4.3]

$$\frac{\partial f(x)}{\partial x} = 0 \ \Rightarrow \ \frac{\partial^2 f(x)}{\partial x^2} \leq 0. \tag{20}$$

Based on lemma 1, we have the following corollary.

Corollary 1: $f(x)$ is a quasi-concave function in $x \in [x_1, x_2]$, if $\frac{\partial f(x)}{\partial x}|_{x=x_1} > 0$, $\frac{\partial f(x)}{\partial x}|_{x=x_2} < 0$ and there is only one maximum over $[x_1, x_2]$ (despite constant functions).

Proposition 1: $\phi(\lambda)$ is a quasiconcave function of λ in the feasible set $0 < \lambda \leq 1$ and the optimal point is given by

$$\lambda_E^\star = \begin{cases} \frac{b_L d_L (c_L - a_L) + \sqrt{-a_L b_L c_L d_L (b_L - d_L)(a_L d_L - b_L c_L - b_L + d_L)}}{a_L b_L (c_L + 1) - c_L d_L (a_L + 1)} & ; \nu \gg 1 \\ 1 - \sqrt{\frac{a_S (c_S + 1)(b_S + c_S + 1)}{b_S c_S}} & ; \nu \ll 1 \end{cases} \tag{21}$$

Proof: The first-order derivative of $\phi(\lambda)$ on λ is given by

$$\frac{\partial \phi(\lambda)}{\partial \lambda} = \begin{cases} \frac{A_L \lambda^2 + B_L \lambda + C_L}{[(a_L+1)\lambda + b_L]^2 [\lambda + d_L]^2} & ; \nu \gg 1 \\ \frac{A_S \lambda^2 + B_S \lambda + C_S}{[1 + (a_L - 1)\lambda]^2 [\lambda + c_L]^2} & ; \nu \ll 1 \end{cases}, \tag{22}$$

where $A_L = -a_L b_L (c_L + 1) + c_L d_L (a_L + 1)$, $B_L = -2 b_L d_L (a_L - c_L)$, $C_L = -a_L b_L \, {d_L}^2 + {b_L}^2 c_L \, d_L$, $A_S = (-b_L \, (a_L - 1) \, c_L - a_L \, (b_L + 1))$, $B_S = -2 \, c_L \, (a_L + b_L)$ and $C_S = -a_L {c_L}^2 + b_L c_L$. As can be seen from (22), $\frac{\partial \phi(\lambda)}{\partial \lambda} = 0$ leads to two solutions on λ. It is easy to examine that the feasible solution for practical values of k_i^t and k_i^r [22] are derived as (21). According to Corollary 1, we find that $\phi(\lambda)$ is a quasiconcave function in the feasible set.

To make the further analysis tractable, we provide new compact expressions for the OPA in the high SNR regime. In the case of DL, the expressions in (13) are simplified to

$$a_L = \frac{1}{\xi_1 - 1}, \quad b_L = \frac{\tau_1}{(\xi_1 - 1)\nu}, \quad c_L = \frac{1}{\tau_2}, \quad d_L = \frac{\tau_3}{\tau_2 \nu}, \tag{23}$$

and in the case of UL scenario, the expressions in (15) are changed to

$$a_S = \frac{\nu}{\xi_1}, \quad b_S = \frac{\nu}{(\nu - 1)\tau_2}, \quad c_S = \frac{1}{\nu - 1}. \tag{24}$$

By substituting (23) and (24) into (21), the OPA solutions in the high SNR regime can be expressed in the following tractable forms

$$\lambda_{High}^\star = \begin{cases} \frac{\theta_L}{\nu} & ; \mathrm{DL} \\ 1 - \theta_S \nu & ; \mathrm{UL} \end{cases} \tag{25}$$

where $\theta_L = \sqrt{\frac{\tau_3}{\tau_2}(\tau_1 - \tau_3)} + \frac{\tau_3}{\tau_2}(\xi_1 - 1) - \tau_3$ and $\theta_S = \sqrt{\frac{1 + \tau_2}{\xi_1}}$.

IV. Ergodic Secrecy Rate

In this section, we derive the ESR of the proposed secure transmission scheme in each case of DL and UL scenarios. Since it is not straightforward to obtain a closed-form expression for the exact ESR of DL and UL scenarios (the exact ESR includes double integral expressions due to the complicated structures of (21)), we therefore proceed by first deriving new analytical expressions for the ESR in the high SNR regime that can be applied to arbitrary channel fading distributions. Based on these, new closed-form expressions are derived for the ESR in Rayleigh fading channels. Despite prior works in the literature [14], [16]–[21] that investigated the ESR based on perfect hardware assumption in various untrusted relaying networks, we take into account hardware imperfections. The new results in this section generalize the recent results in [14], [17].

The ESR as a useful secrecy metric representing the rate below which any average secure transmission rate is achievable [2]. As such, the ESR is given by

$$\overline{R_s} = \mathbb{E}\Big\{ R_s \Big\} = \frac{1}{2\ln 2}\Big[\underbrace{\mathbb{E}\Big\{ \ln(1+\gamma_{\rm D}) \Big\}}_{T_1} - \underbrace{\mathbb{E}\Big\{ \ln(1+\gamma_{\rm R}) \Big\}}_{T_2} \Big]. \tag{26}$$

In the following, we proceed to evaluate the parts T_1 and T_2 and then $\overline{R_s}$ for each case of DL and UL scenarios. Towards this goal, we present the following useful lemma.

Lemma 2: For positive constants α_1, α_2 and α_3, and non-negative r.v. Γ, the cdf of the new r.v. $\widehat{\Gamma} = \frac{\alpha_1\Gamma}{\alpha_2\Gamma+\alpha_3}$ is derived as

$$F_{\widehat{\Gamma}}(x) = \begin{cases} F_{\Gamma}\Big(\frac{\alpha_3 x}{\alpha_1-\alpha_2 x}\Big) & ; 0 \le x < \frac{\alpha_1}{\alpha_2} \\ 1 & ; x \ge \frac{\alpha_1}{\alpha_2} \end{cases} \tag{27}$$

Proof: We start from the definition of the cdf as follows

$$F_{\widehat{\Gamma}}(x) = \Pr\Big\{ \frac{\alpha_1\Gamma}{\alpha_2\Gamma+\alpha_3} \le x \Big\} = \Pr\Big\{ \Gamma(\alpha_1-\alpha_2 x) \le \alpha_3 x \Big\}, \tag{28}$$

where the last probability equals to one for $\alpha_1 - \alpha_2 x < 0$. Otherwise, it equals to $F_{\Gamma}\Big(\frac{\alpha_3 x}{\alpha_1-\alpha_2 x}\Big)$.

1) Downlink Scenario: By plugging (25) into (12), we obtain

$$\gamma_{\mathrm{R}} = \frac{\theta_L}{\theta_L(\xi_1 - 1) + \tau_1}, \tag{29}$$

$$\gamma_{\mathrm{D}} = \frac{\theta_L \gamma_{\mathrm{rd}}}{(\tau_2\theta_L + \tau_3)\gamma_{\mathrm{rd}} + \xi_1\theta_L + \tau_4}. \tag{30}$$

We find that all the terms in (29) and (30) are deterministic constants which leads to the secrecy rate ceiling in the high SNR regime.

Based on lemma 2 and (30), the part T_1 in (26) is given by

$$T_1 = \mathbb{E}\Big\{ \ln\Big(1 + \frac{\theta_L \gamma_{\mathrm{rd}}}{(\tau_2\theta_L + \tau_3)\gamma_{\mathrm{rd}} + \xi_1\theta_L + \tau_4}\Big)\Big\} = \int_0^{\frac{\theta_L}{\tau_2\theta_L + \tau_3}} \frac{1 - F_{\gamma_{\mathrm{rd}}}\Big(\frac{(\xi_1\theta_L + \tau_4)x}{\theta_L - (\tau_2\theta_L + \tau_3)x}\Big)}{1 + x}\mathrm{d}x, \tag{31}$$

where the last equation follows from the integration by parts. The expression in (31) is straightforwardly evaluated for any channel fading distribution, either directly or by a simple numerical integration.

Furthermore, based on (30) the part T_2 is a constant value as

$$T_2 = \ln\Big(1 + \frac{\theta_L}{\theta_L(\xi_1 - 1) + \tau_1}\Big). \tag{32}$$

We conclude from (32) that the amount of information leakage is independent of the transmit SNR and the position of the relay, and only depends on the EVMs at network nodes. By replacing (31) and (32) into (26), the compact ESR expression is achieved for any channel distribution.

For the case of Rayleigh fading, due to the fact that γ_{rd} is an exponential r.v. and applying [34, Eq. (4.337.2)], the part T_1 can be expressed in a closed-form solution. By substituting this and (32) into (26), the closed-form ESR expression becomes

$$\overline{R_s}^{\mathrm{DL}} = \frac{1}{2\ln 2}\Big[e^{\frac{1}{r_2\overline{\gamma}_{\mathrm{rd}}}}\mathrm{Ei}(-\frac{1}{r_2\overline{\gamma}_{\mathrm{rd}}}) - e^{\frac{1}{r_1\overline{\gamma}_{\mathrm{rd}}}}\mathrm{Ei}(-\frac{1}{r_1\overline{\gamma}_{\mathrm{rd}}}) - \ln\Big(1 + \frac{\theta_L}{\theta_L(\xi_1 - 1) + \tau_1}\Big)\Big], \tag{33}$$

where $r_1 = \frac{(1+\tau_2)\theta_L + \tau_3}{\xi_1\theta_L + \tau_4}$ and $r_2 = \frac{\tau_2\theta_L + \tau_3}{\xi_1\theta_L + \tau_4}$. We conclude from (33) that the ESR is exclusively characterized by the level of imperfections over nodes and $\overline{\gamma}_{\mathrm{rd}}$ which is a function of the transmit SNR and the distance-dependent channel gain μ_{rd}.

2) Uplink Scenario: Substituting (25) into (14) yields

$$\gamma_{\rm R} = \frac{\lambda_{\rm H}^{\star}\nu}{(1-\lambda_{\rm H}^{\star})\xi_1} \approx \frac{1}{\sqrt{\xi_1(1+\tau_2)}}, \tag{34}$$

$$\gamma_{\rm D} \approx \frac{\gamma_{\rm sr}}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})\gamma_{\rm sr}+\xi_2-\xi_1}. \tag{35}$$

Observe from (34) and (35) that only the first hop SNR, $\gamma_{\rm sr}$ contributes to the secrecy rate performance. Following the similar procedure as the DL scenario, the ESR performance of the UL case for arbitrary fading distribution can be expressed as

$$\overline{R_s}^{\rm UL} = \frac{1}{2\ln 2}\Big(\int_0^{\frac{1}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}} \frac{1-F_{\gamma_{\rm sr}}(\frac{(\xi_2-\xi_1)x}{1-\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})x})}{1+x}\,{\rm d}x - \ln(1+\frac{1}{\sqrt{\xi_1(1+\tau_2)}})\Big). \tag{36}$$

For the case of Rayleigh fading, the closed-form ESR expression is given by

$$\overline{R_s}^{\rm UL} = \frac{1}{2\ln 2}\Big[e^{\frac{1}{t_2\overline{\gamma}_{\rm sr}}}{\rm Ei}(-\frac{1}{t_2\overline{\gamma}_{\rm sr}}) - e^{\frac{1}{t_1\overline{\gamma}_{\rm sr}}}{\rm Ei}(-\frac{1}{t_1\overline{\gamma}_{\rm sr}}) - \ln\Big(1+\frac{1}{\sqrt{\xi_1(1+\tau_2)}}\Big)\Big], \tag{37}$$

where $t_1 = \frac{1+\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}{\xi_2-\xi_1}$ and $t_2 = \frac{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}{\xi_2-\xi_1}$. It is observed from (37) that the ESR is entirely determined by the average channel gain of the first hop, the transmit SNR and the level of imperfections of all the network nodes. We also find that increasing the number of antennas at D has no impact on the ESR when $N_{\rm d}$ is large.

V. Secrecy Outage Probability

In this section, similar to our ESR results, general expressions are first presented for the SOP that can be applied to any channel distribution, under the presence of transceiver imperfections and in the high SNR regime. Based on these, we derive novel closed-form expressions for the SOP in Rayleigh fading channels.

The SOP denoted by $P_{\rm so}$ is a criterion that determines the fraction of fading realizations where a secrecy rate R_t cannot be supported [13]. Accordingly, the overall SOP is defined as the probability that a system with the instantaneous secrecy rate R_s is not able to support the target transmission rate R_t; $P_{\rm so} = \Pr\Big\{R_s < R_t\Big\}$.

In the following, we focus on each case of DL and UL, respectively.

1) Downlink Scenario: Substituting (30) into (17) and then based on the SOP definition we obtain

$$P_{\rm so}^{\rm DL} = \Pr\left(\frac{\theta_L\gamma_{\rm rd}}{(\tau_2\theta_L+\tau_3)\gamma_{\rm rd}+\xi_1\theta_L+\tau_4} \leq \widetilde{R_t}\right) = \begin{cases} F_{\gamma_{\rm rd}}\left(\frac{(\xi_1\theta_L+\tau_4)\widetilde{R_t}}{\theta_L-(\tau_2\theta_L+\tau_3)\widetilde{R_t}}\right) & ; R_t < \frac{1}{2}\log_2\left(\frac{1+\frac{\theta_L}{\tau_2\theta_L+\tau_3}}{1+\gamma_{\rm R}}\right) \\ 1 & ; R_t \geq \frac{1}{2}\log_2\left(\frac{1+\frac{\theta_L}{\tau_2\theta_L+\tau_3}}{1+\gamma_{\rm R}}\right) \end{cases} \tag{38}$$

where $\widetilde{R_t} = 2^{2R_t}(1+\gamma_{\rm R})-1$ and $\gamma_{\rm R}$ is in (29), and the last equation follows from using lemma 2. It is worth pointing out that the SOP expressions in (38) allows the straightforward evaluation of the SOP for any channel fading distribution by a simple numerical integration. We can conclude from (38) that the SOP is always 1 for target transmission rates more than a threshold (which only depends on the EVMs of the nodes). Interestingly, this event holds for any channel fading distribution, any network topology and any transmit SNR. Therefore as explained in Section IV, some secrecy rates can never be achieved due to secrecy rate ceiling. Furthermore, we conclude that for target transmission rates smaller than the threshold, $P_{\rm so}$ approaches zero with increasing SNR (similar to perfect hardware) whereas the SOP always equals one for target transmission rates larger than the threshold. This result is fundamentally different to the perfect hardware case where the SOP goes to zero with increasing SNR and for any target transmission rate [13], [15], [17].

For Rayleigh fading channels, $\gamma_{\rm rd}$ is an exponential r.v. and therefore, our new and simple closed-form SOP expression in the presence of transceiver hardware imperfection is given by

$$P_{\rm so}^{\rm DL} = \begin{cases} 1-\exp\left(-\frac{(\xi_1\theta_L+\tau_4)\widetilde{R_t}}{(\theta_L-(\tau_2\theta_L+\tau_3)\widetilde{R_t})\overline{\gamma}_{\rm rd}}\right) & ; R_t < \frac{1}{2}\log_2\left(\frac{1+\frac{\theta_L}{\tau_2\theta_L+\tau_3}}{1+\gamma_{\rm R}}\right) \\ 1 & ; R_t \geq \frac{1}{2}\log_2\left(\frac{1+\frac{\theta_L}{\tau_2\theta_L+\tau_3}}{1+\gamma_{\rm R}}\right) \end{cases} \tag{39}$$

We note that the results of this section generalize the results of [17] which were derived for the case of untrusted relaying with perfect hardware.

2) Uplink Scenario: Similar to the DL case, the SOP can be obtained by substituting $\gamma_{\rm D}$ in

(35) into (17) and using the SOP definition. This yields

$$P_{\rm so}^{\rm UL}=\begin{cases} F_{\gamma_{\rm sr}}\Big(\frac{(\xi_2-\xi_1)\widetilde{R_t}}{1-\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})\widetilde{R_t}}\Big) & ;R_t<\frac{1}{2}\log_2\Big(\frac{1+\frac{1}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}}{1+\gamma_{\rm R}}\Big) \\ 1 & ;R_t\geq\frac{1}{2}\log_2\Big(\frac{1+\frac{1}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}}{1+\gamma_{\rm R}}\Big) \end{cases} \tag{40}$$

where $\widetilde{R_t}=2^{2R_t}(1+\gamma_{\rm R})-1$ and $\gamma_{\rm R}$ is in (34). For the special case of Rayleigh fading channels, the closed-form SOP is derived as

$$P_{\rm so}^{\rm UL}=\begin{cases} 1-\exp\Big(\frac{-(\xi_2-\xi_1)\widetilde{R_t}}{(1-\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})\widetilde{R_t})\overline{\gamma}_{\rm sr}}\Big) & ;R_t<\frac{1}{2}\log_2\Big(\frac{1+\frac{1}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}}{1+\gamma_{\rm R}}\Big) \\ 1 & ;R_t\geq\frac{1}{2}\log_2\Big(\frac{1+\frac{1}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})}}{1+\gamma_{\rm R}}\Big) \end{cases} \tag{41}$$

As observed in the numerical results, the closed-form expressions (39) and (41) are sufficiently tight at medium and high transmit SNRs.

VI. Hardware Design

In this section, we aim to gain some insights into the design of RF hardware to maximize the secrecy rate in untrusted relaying networks. Depending on the fixed cost of each network node, we show how the RF segments at the transmission and reception front ends can be designed. Specially, given the maximum tolerable hardware imperfection of each node, we derive new analytical results characterizing how the hardware imperfections should be distributed between the transmission RF segment and the reception RF segment of each node to maximize the secrecy rate. Therefore, we should find k_i^t and k_i^r, $i\in\{\rm S,R,D\}$ to maximize the secrecy rate such that $k_i^t+k_i^r=k_i^{\rm tot}$. Mathematically speaking, our goal is to solve the following optimization problem

$$\begin{aligned}(k_{\rm R}^t,k_{\rm R}^r,k_{\rm D}^t,k_{\rm D}^r)=\arg\quad&\max\phi(\lambda^\star)\\ \text{s.t. }\ &k_{\rm R}^t+k_{\rm R}^r=k_{\rm R}^{\rm tot}\\ &k_{\rm D}^t+k_{\rm D}^r=k_{\rm D}^{\rm tot}\end{aligned} \tag{42}$$

Based on (30), (35) and (17), the instantaneous secrecy rate is an increasing function of the transmit SNR. Since it is our aim to achieve high transmission rates, we consider the asymptotic SNR regime $\rho\to\infty$ [22] to solve the hardware design problem (42). As observed in numerical studies, the results of the high SNR analysis can be applied successfully at finite SNRs.

In the asymptotic SNR regime and for any random distributions on $\gamma_{\rm sr}$ and $\gamma_{\rm rd}$, the asymptotic received SNDRs at R and D are respectively, given by

$$\gamma_{\rm R}^{\infty} = \begin{cases} \frac{\theta_L}{\theta_L(\xi_1-1)+\tau_1} & ;\mathrm{DL} \\ \frac{1}{\sqrt{\xi_1(1+\tau_2)}} & ;\mathrm{UL} \end{cases}, \tag{43}$$

and

$$\gamma_{\rm D}^{\infty} = \begin{cases} \frac{\theta_L}{\tau_2\theta_L+\tau_3} & ;\mathrm{DL} \\ \frac{1}{\tau_2(1+\sqrt{\frac{1+\tau_2}{\xi_1}})} & ;\mathrm{UL} \end{cases}. \tag{44}$$

By substituting (43) and (44) into (18), the secrecy rate ceiling is given by

$$\phi^{\infty} = \begin{cases} \frac{((1+\tau_2)\theta_L+\tau_3)((\xi_1-1)\theta_L+\tau_1)}{(\xi_1\theta_L+\tau_1)(\tau_2\theta_L+\tau_3)} & ;\mathrm{DL} \\ \frac{\sqrt{\xi_1}(\tau_2+1)\left(\tau_2+\sqrt{\xi_1}\sqrt{\tau_2+1}\right)}{\tau_2\left(\sqrt{\xi_1}+\sqrt{\tau_2+1}\right)\left(\sqrt{\xi_1}\sqrt{\tau_2+1}+1\right)} & ;\mathrm{UL} \end{cases} \tag{45}$$

Some conclusions and insights can be concluded from (45). First, the secrecy rate ceiling event appears in the asymptotic SNR regime, which significantly limits the performance of the system. This event is different from the perfect hardware case, in which the ESR increases with increasing SNR. Note that this ceiling effect is independent of the fading distribution.

In the following, we focus on the of DL and UL scenarios separately and then conclude about the hardware design of the overall network.

A. Downlink Scenario:

In the following, we proceed to solve the optimization problem (42) by independently discussing on the hardware design at R and D as follows.

Proposition 2: Suppose $k_{\rm R}^t + k_{\rm R}^r = k_{\rm R}^{\rm tot}$, hence the secrecy rate ceiling is maximized if $k_{\rm R}^t = k_{\rm R}^r = \frac{k_{\rm R}^{\rm tot}}{2}$.

Proof: Please see Appendix A.

Proposition 3: Suppose $k_{\rm D}^t + k_{\rm D}^r = k_{\rm D}^{\rm tot}$, thus the secrecy rate ceiling is maximized if

$$k_{\rm D}^t = \frac{2k_{\rm R}^2+2{k_{\rm D}^{\rm tot}}^2+3-\sqrt{4k_{\rm R}^4+8k_{\rm R}^2{k_{\rm D}^{\rm tot}}^2+4{k_{\rm D}^{\rm tot}}^4+12k_{\rm R}^2-4{k_{\rm D}^{\rm tot}}^2+9}}{4k_{\rm D}^{\rm tot}}. \tag{46}$$

Proof: Please see Appendix B.

B. Uplink Scenario:

Similar to DL scenario, two propositions are provided as follows.

Proposition 4: Suppose $k_{\mathrm{R}}^{t}+k_{\mathrm{R}}^{r}=k_{\mathrm{R}}^{\mathrm{tot}}$, thus the secrecy rate ceiling is maximized if $k_{\mathrm{R}}^{t}=k_{\mathrm{R}}^{r}=\frac{k_{\mathrm{R}}^{\mathrm{tot}}}{2}$.

Proof: Please see Appendix C.

Proposition 5: Suppose $k_{\mathrm{D}}^{t}+k_{\mathrm{D}}^{r}=k_{\mathrm{D}}^{\mathrm{tot}}$, hence the secrecy rate ceiling is a monotonically decreasing function of k_{D}^{r}.

Proof: In this case, we have

$$\frac{\partial\phi^{\infty}}{\partial k_{\mathrm{D}}^{r}}=\frac{\partial\phi^{\infty}}{\partial\tau_{2}}\frac{\partial\tau_{2}}{\partial k_{\mathrm{D}}^{r}}, \tag{47}$$

where $\frac{\partial\tau_{2}}{\partial k_{\mathrm{D}}^{r}}=2{k_{\mathrm{R}}^{r}}^{2}k_{\mathrm{D}}^{r}+2k_{\mathrm{D}}^{r}>0$ and $\frac{\partial\phi^{\infty}}{\partial\tau_{2}}$ in (67) is negative in the feasible set. As such, $\frac{\partial\phi^{\infty}}{\partial k_{\mathrm{D}}^{r}}<0$.

Based on Propositions 2–5, we provide the following corollary as a conclusion of the analysis which provides new insights into the system design.

Corollary 2: Consider a cooperative network in which one multiple antennas node communicates with a single antenna node via a single antenna untrusted relay. Let us assume a predefined cost can be assigned to each node. To maximize the secrecy rate of this network the following considerations should be taken into account:

- According to Propositions 2 and 4, the total cost for the relay node should be divided by half between the transmission and reception RF front ends, i,e., it is better to apply the same level of imperfections at every transceiver chain, instead of utilizing a mix of high-quality and low-quality transceiver chains.
- According to Proposition 5, to design the multiple antennas node, the designers are persuaded to use higher-quality hardware in reception RF front end and lower-quality hardware

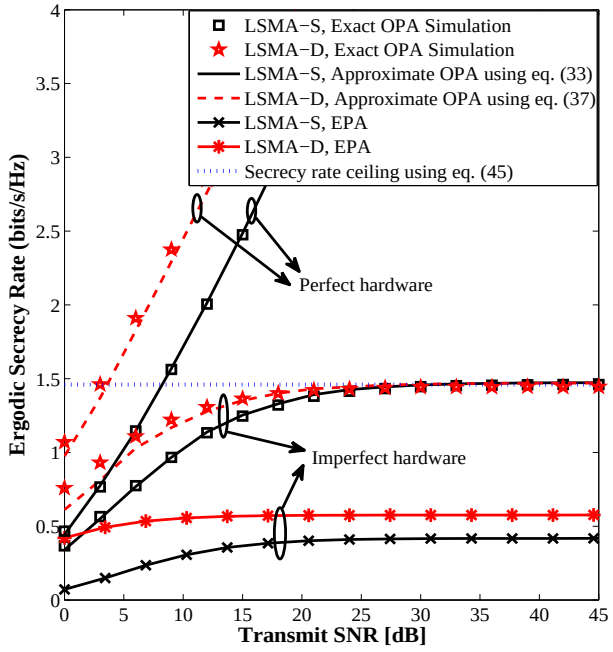

Fig. 2. Ergodic secrecy rate versus transmit SNR for exact and the derived closed-form expressions under perfect and imperfect transceiver hardwares. Number of antennas at source or destination is set to 16. For imperfect case with $k = 0.1$, the secrecy rate ceiling is observed.

in the transmission RF front end, i.e, the hardware imperfections at the reception end of the multiple antennas node should be close to zero.

- According to Proposition 3, to design the single antenna node, the quality of RF requirements at the transmission end should obeys from (46). As observed in the numerical examples, we obtain $k_{\mathrm{D}}^{t} > \frac{k_{\mathrm{D}}^{\mathrm{tot}}}{2}$ for typical values of EVMs.

VII. Numerical Results and Discussions

In this section, numerical results are provided to verify the accuracy of the derived closed-form expressions in Section IV and V for LSMA at S (LSMA-S) and LSMA at D (LSMA-D), respectively, and also the cases of multiple antennas at S (MA-S) and multiple antennas at D (MA-D). We compare our LSMA-based ESR performance with the exact ESR with Monte-Carlo simulations where the OPA is numerically evaluated for finite numbers of antennas using the bisection method. In addition, the equal power allocation (EPA) between S and D (i.e., $\lambda = 0.5$) is plotted as a benchmark. Furthermore, the concepts of secrecy rate ceiling and the practical hardware insights from Section VI are numerically presented. In our numerical evaluations, the

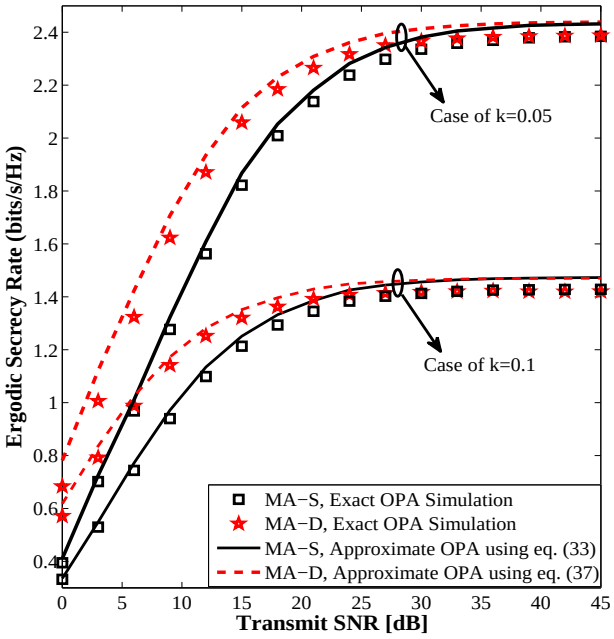

Fig. 3. Ergodic secrecy rate versus transmit SNR for exact and the derived closed-form expressions under different levels of hardware imperfections; $k \in \{0.05, 0.1\}$. Number of antennas at source or destination is set to 4.

transmission links between nodes are modeled by the Rayleigh fading channel and the average channel gains are specified as $\mu_{\rm sr} = \mu_{\rm rd} = 10$. Moreover, for LSMA the number of antennas is set to 16, and for MA the number of antennas is set to 4.

Fig. 2 depicts the ESR versus transmit SNR ρ in dB for both cases of DL and UL and for perfect ($k = k_{\rm R}^t = k_{\rm R}^r = k_{\rm S}^t = k_{\rm D}^t = k_{\rm D}^r = 0$) and imperfect ($k = 0.1$) cases. The number of antennas at S and D are set to $N_{\rm s} = N_{\rm d} = 16$. It is observed from the figure that the Monte-Carlo simulation of the exact OPA evaluated using the bisection method is in good agreement with the derived high SNR closed-form solutions in (33) and (37) for both perfect and imperfect hardwares. In contrast to perfect hardware, the figure shows that the ESR ceiling phenomenon occurs for imperfect hardware which reveals the performance limits of hardware-constrained realistic networks in the high SNR regime. This figure also reveals that hardware imperfections have low impact at low SNRs, but are significant in the high SNR regime. Furthermore, it is observed that the proposed OPA increases the secrecy rate floor by approximately 1 bits/s/Hz and 0.9 bits/s/Hz for DL and UL scenarios, respectively compared to the EPA ($\lambda = 0.5$).

In Fig. 3, we examine the accuracy of the derived closed-form solutions for MA-S and MA-D by considering $N_{\rm s} = N_{\rm d} = 4$. As can be seen, the numerical and the theoretical curves are in

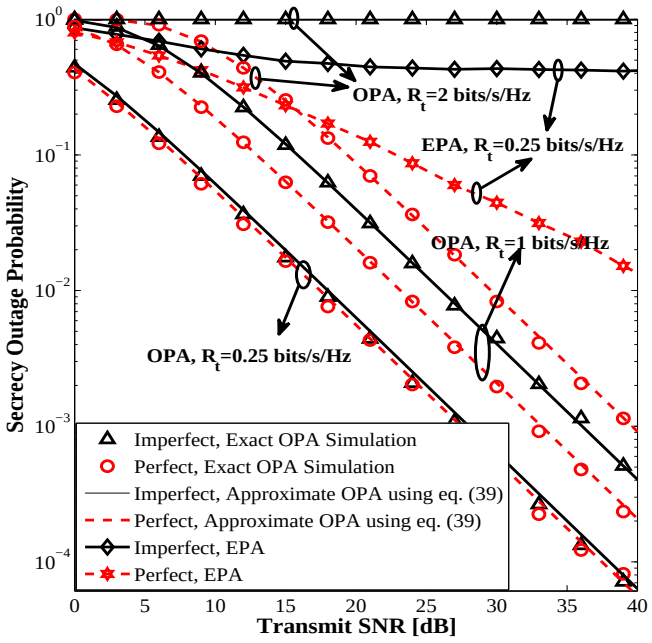

Fig. 4. Secrecy outage probability versus transmit SNR for DL transmission, with different target transmission rates and under perfect $(k = 0)$ and imperfect hardware $(k = 0.1)$.

good agreement across all SNR regimes. Moreover, it is observed that by increasing the level of hardware imperfections from $k = 0.05$ to $k = 0.1$, the achievable secrecy rate is degraded approximately 1 bits/s/Hz in the high SNR regime.

Figs. 4 and 5 show the SOP as a function of the transmit SNR for LSMA based DL and UL scenarios, respectively, and for different target secrecy rates. The theoretical curves were plotted by the derived analytical expressions in (39) and (41) which are well-tight with the marker symbols generated by the Monte-Carlo simulations. As observed from these figures, there is only a negligible performance loss caused by transceiver hardware imperfections in the low target secrecy rate of $R_t = 0.25$ bits/s/Hz, but by increasing the target secrecy rate to $R_t = 1$ bits/s/Hz or $R_t = 2$ bits/s/Hz, substantial performance loss is revealed. Interestingly, for $R_t = 2$ bits/s/Hz, the network with imperfect hardware is always in outage and secure communications is unattainable-irrespective of the transmit SNR. This is exactly predicted by our analytical results in section V. The reason is that this target secrecy rate is more than the derived thresholds in (39) and (41), and as mentioned, the SOP of the system always equals one for R_t more the thresholds. It can also be seen from the figures that despite the OPA technique that the SOP curves with imperfect hardware and with perfect hardware have the same slope (and thus,

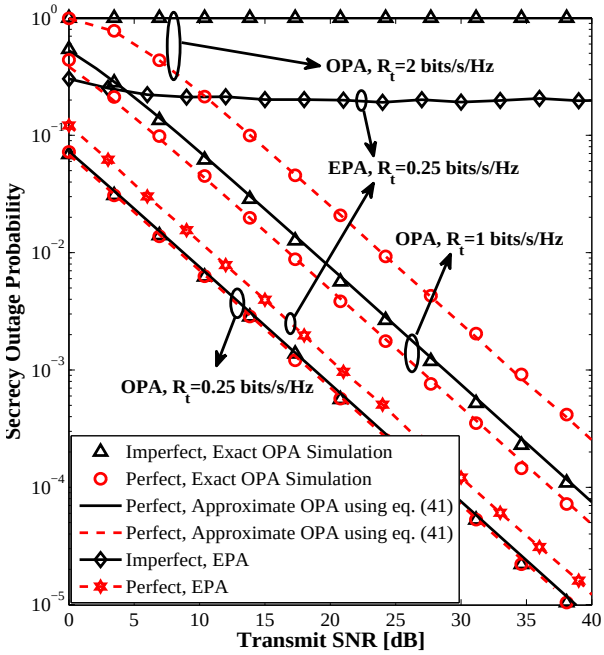

Fig. 5. Secrecy outage probability versus transmit SNR for UL transmission, with different target transmission rates and under perfect $(k = 0)$ and imperfect hardware $(k = 0.1)$.

hardware imperfections lead to only an SNR offset which is unveiled as a curve shifting to the right), the SOP performance of the EPA technique approaches a non-zero saturation value in the high SNR regime for imperfect hardware. This observation reveals the secrecy performance advantage of the proposed OPA scheme compared with EPA.

Finally, we provide Figs. 6 and 7 to illustrate the insights for designing practical systems that were presented in Section VI. In the simulation, we assume that the total hardware imperfection over each node equals to 0.2, i.e., $k_{\mathrm{R}}^{\mathrm{tot}} = k_{\mathrm{D}}^{\mathrm{tot}} = 0.2$. Based on Propositions 2 and 4, to maximize the secrecy rate, we should design the transmission and reception RF front ends at R such that $k_{\mathrm{R}}^{t} = k_{\mathrm{R}}^{r} = 0.1$. For LSMA at S, based on Proposition 3, we obtain $k_{\mathrm{D}}^{t} = 0.13$ and $k_{\mathrm{D}}^{r} = 0.07$ while for LSMA at D and based on Proposition 5, we should design the hardwares such that $k_{\mathrm{D}}^{t} = 0.2$ and $k_{\mathrm{D}}^{r} = 0$. By defining the hardware imperfection vector as $\mathrm{IV} = [k_{\mathrm{R}}^{t}, k_{\mathrm{R}}^{r}, k_{\mathrm{D}}^{t}, k_{\mathrm{D}}^{r}]$, we consider the following four different hardware design schemes:

- Design 1: R and D are designed randomly, for example IV$= [0.15, 0.05, 0.1, 0.1]$,
- Design 2: R is designed optimally based on Propositions 2 and 4 while D is designed randomly; IV$= [0.1, 0.1, 0.1, 0.1]$,
- Design 3: R is designed randomly while D is designed optimally; For LSMA at S, IV$=$

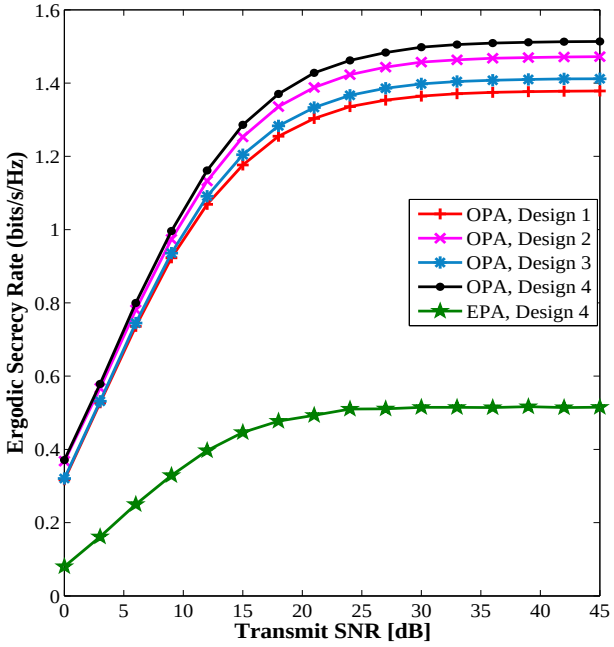

Fig. 6. Ergodic secrecy rate versus transmit SNR for LSMA at S. Various imperfection distributions over RF transmission and reception ends are considered for $k_{\mathrm{R}}^{\mathrm{tot}} = k_{\mathrm{D}}^{\mathrm{tot}} = 0.2$.

$[0.15, 0.05, 0.13, 0.07]$ and for LSMA at D, IV$= [0.15, 0.05, 0.2, 0]$, and

- Design 4: R and D are designed optimally; For LSMA at S, IV$= [0.1, 0.1, 0.13, 0.07]$ and for LSMA at D, IV$= [0.1, 0.1, 0.2, 0]$.

The results depict that the hardware design 4 which is based on Propositions 2-5 provides higher ESR performance compared to the case of random hardware design (Design 1) and the cases of optimizing only one node (Designs 2 and 3). Furthermore, they show that the analysis presented in Section VI (which was based on high SNR analysis), can be utilized auspiciously at medium SNRs. In addition, as can be seen from these figures and mentioned before, different hardware designs have the ESR performance close together at low SNR regime, while the difference between the ESR performance of the designs is large at high SNR regime. Finally, we can understand from the figure that the proposed OPA together with Design 4 significantly outperforms the scenario of EPA with Design 4.

VIII. Conclusion

Physical radio-frequency (RF) transceivers are inseparable segments in both traditional and new emerging wireless networks. In the literature, very few works have considered the impact

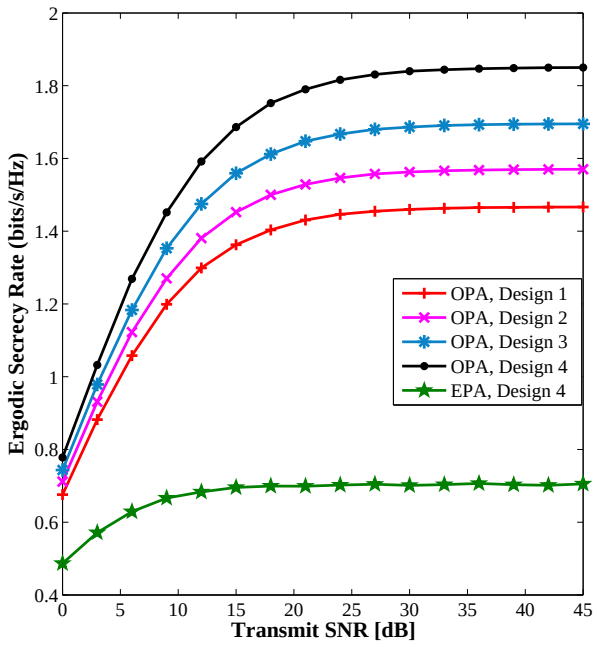

Fig. 7. Ergodic secrecy rate versus transmit SNR for LSMA at D. Various imperfection distributions over RF transmission and reception ends are considered for $k_{\mathrm{R}}^{\mathrm{tot}} = k_{\mathrm{D}}^{\mathrm{tot}} = 0.2$.

of hardware imperfections on security based transmissions and little is understood regarding this impact on untrusted relaying networks. In this paper, by taking hardware imperfections into consideration, we proposed an optimal power allocation (OPA) strategy to maximize the instantaneous secrecy rate of a cooperative wireless network comprised of a source, a destination and an untrusted amplify-and-forward (AF) relay. Based on our OPA solutions, new closed-form expressions were derived for the ergodic secrecy rate (ESR) and secrecy outage probability (SOP) with Rayleigh fading channels. The expressions effectively characterize the impact of hardware imperfections and manifest the existence of a secrecy rate ceiling that cannot be enhanced by increasing SNR or improving fading conditions. They also illustrate that hardware imperfections have low impact at low SNRs, but are significant in the high SNR regime. This issue reveals that hardware imperfections should be taken into account when developing high rate systems such as LTE-Advanced and 5G networks. To improve the secrecy performance of the network, we finally presented the hardware design approach. Numerical results depict that optimally distributing the hardware imperfections between the transmission and reception RF segments can further improve the secrecy performance.

APPENDIX A

Let take the first-order derivative of ϕ^{∞} on k_{R}^{t} using the chain rule in partial derivations as follows

$$\frac{\partial \phi^{\infty}}{\partial k_{\mathrm{R}}^{t}} = \frac{\partial \phi^{\infty}}{\partial \theta_L}\Big(\frac{\partial \theta_L}{\partial \tau_1}\frac{\partial \tau_1}{\partial k_{\mathrm{R}}^{t}} + \frac{\partial \theta_L}{\partial \tau_2}\frac{\partial \tau_2}{\partial k_{\mathrm{R}}^{t}} + \frac{\partial \theta_L}{\partial \tau_3}\frac{\partial \tau_3}{\partial k_{\mathrm{R}}^{t}} + \frac{\partial \theta_L}{\partial \xi_1}\frac{\partial \xi_1}{\partial k_{\mathrm{R}}^{t}}\Big) + \frac{\partial \phi^{\infty}}{\partial \tau_1}\frac{\partial \tau_1}{\partial k_{\mathrm{R}}^{t}} + \frac{\partial \phi^{\infty}}{\partial \tau_2}\frac{\partial \tau_2}{\partial k_{\mathrm{R}}^{t}} + \frac{\partial \phi^{\infty}}{\partial \tau_3}\frac{\partial \tau_3}{\partial k_{\mathrm{R}}^{t}} + \frac{\partial \phi^{\infty}}{\partial \xi_1}\frac{\partial \xi_1}{\partial k_{\mathrm{R}}^{t}}, \tag{48}$$

where using (45), we obtain

$$\frac{\partial \phi^{\infty}}{\partial \theta_L} = \frac{\kappa_1 {\theta_L}^2 + \kappa_2 \theta_L + \kappa_3}{(\theta_L \xi_1 + \tau_1)^2 (\tau_2 \theta_L + \tau_3)^2}, \tag{49}$$

$$\frac{\partial \theta_L}{\partial \tau_1} = \frac{\tau_3}{2\sqrt{\tau_2 \tau_3 \left(\tau_1 - \tau_3\right)}}, \tag{50}$$

$$\frac{\partial \theta_L}{\partial \tau_2} = -\frac{\sqrt{\tau_3(\tau_1 - \tau_3)}}{2\tau_2\sqrt{\tau_2}} - \frac{\tau_3(\xi_1 - 1)}{\tau_2^2}, \tag{51}$$

$$\frac{\partial \theta_L}{\partial \tau_3} = \frac{\tau_1 - 2\tau_3}{2\sqrt{\tau_2 \tau_3 (\tau_1 - \tau_3)}} + \frac{\xi_1 - 1}{\tau_2} - 1, \tag{52}$$

$$\frac{\partial \theta_L}{\partial \xi_1} = \frac{\tau_3}{\tau_2}, \tag{53}$$

$$\frac{\partial \phi^{\infty}}{\partial \tau_1} = \frac{\theta_L \left(\tau_2 \theta_L + \tau_3 + \theta_L\right)}{\left(\theta_L \xi_1 + \tau_1\right)^2 \left(\tau_2 \theta_L + \tau_3\right)}, \tag{54}$$

$$\frac{\partial \phi^{\infty}}{\partial \tau_2} = -\frac{\theta_L^2(\xi_1 \theta_L + \tau_1 - \theta_L)}{(\tau_2 \theta_L + \tau_3)^2(\xi_1 \theta_L + \tau_1)}, \tag{55}$$

$$\frac{\partial \phi^{\infty}}{\partial \tau_3} = -\frac{\theta_L(\xi_1 \theta_L + \tau_1 - \theta_L)}{(\tau_2 \theta_L + \tau_3)^2(\xi_1 \theta_L + \tau_1)}, \tag{56}$$

$$\frac{\partial \phi^{\infty}}{\partial \xi_1} = \frac{\theta_L^2(\tau_2 \theta_L + \tau_3 + \theta_L)}{(\xi_1 \theta_L + \tau_1)^2(\tau_2 \theta_L + \tau_3)}, \tag{57}$$

where $\kappa_1 = -\tau_1\tau_2(\tau_2+1) + \tau_3\xi_1(\xi_1-1)$, $\kappa_2 = -2\tau_1\tau_3(\tau_2-\xi_1+1)$ and $\kappa_3 = \tau_1\tau_3(\tau_1-\tau_3)$. By substituting $k_{\mathrm{R}}^r = k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t$ into (45), we obtain

$$\frac{\partial\tau_1}{\partial k_{\mathrm{R}}^t} = -2k_{\mathrm{R}}^{\mathrm{tot}} + 2k_{\mathrm{R}}^t, \tag{58}$$

$$\frac{\partial\tau_2}{\partial k_{\mathrm{R}}^t} = -2{k_{\mathrm{D}}^r}^2(k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t) - 2(k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t){k_{\mathrm{R}}^t}^2 + 2(k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t)^2k_{\mathrm{R}}^t + 4k_{\mathrm{R}}^t - 2k_{\mathrm{R}}^{\mathrm{tot}}, \tag{59}$$

$$\frac{\partial\tau_3}{\partial k_{\mathrm{R}}^t} = -2{k_{\mathrm{D}}^r}^2(k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t) - 2(k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t){k_{\mathrm{R}}^t}^2 + 2(k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^t)^2k_{\mathrm{R}}^t + 4k_{\mathrm{R}}^t - 2k_{\mathrm{R}}^{\mathrm{tot}} + 2k_{\mathrm{R}}^t{k_{\mathrm{D}}^t}^2, \tag{60}$$

$$\frac{\partial\xi_1}{\partial k_{\mathrm{R}}^t} = -2k_{\mathrm{R}}^{\mathrm{tot}} + 2k_{\mathrm{R}}^t. \tag{61}$$

Substituting (49)–(61) into (48) and after tedious manipulations yields

$$\frac{\partial\phi^\infty}{\partial k_{\mathrm{R}}^t} = \frac{4(1-{k_{\mathrm{D}}^r}^2)(k_{\mathrm{R}}^{\mathrm{tot}} - 2k_{\mathrm{R}}^t)}{\left(4{k_{\mathrm{R}}^t}^2 - 4k_{\mathrm{R}}^tk_{\mathrm{R}}^{\mathrm{tot}} + 2{k_{\mathrm{R}}^{\mathrm{tot}}}^2 + 2{k_{\mathrm{D}}^r}^2 + {k_{\mathrm{D}}^t}^2\right)^2}. \tag{62}$$

Expression (62) shows that ϕ^∞ is a concave function of k_{R}^t in the feasible set and $k_{\mathrm{R}}^t = \frac{k_{\mathrm{R}}^{\mathrm{tot}}}{2}$ is the single solution to $\frac{\partial\phi^\infty}{\partial k_{\mathrm{R}}^t} = 0$.

APPENDIX B

Following the similar approach in Proposition 2, we should evaluate $\frac{\partial\phi^\infty}{\partial k_{\mathrm{D}}^t}$. Let substitute $k_{\mathrm{D}}^r = k_{\mathrm{D}}^{\mathrm{tot}} - k_{\mathrm{D}}^t$ into τ_1, τ_2, τ_3 and then compute the following derivations

$$\frac{\partial\tau_1}{\partial k_{\mathrm{D}}^t} = 1, \quad \frac{\partial\tau_2}{\partial k_{\mathrm{D}}^t} = -2{k_{\mathrm{R}}^r}^2(k_{\mathrm{D}}^{\mathrm{tot}} - k_{\mathrm{D}}^t) - 2k_{\mathrm{D}}^{\mathrm{tot}} + 2k_{\mathrm{D}}^t, \tag{63}$$

$$\frac{\partial\tau_3}{\partial k_{\mathrm{D}}^t} = -2{k_{\mathrm{R}}^r}^2(k_{\mathrm{D}}^{\mathrm{tot}} - k_{\mathrm{D}}^t) - 2k_{\mathrm{D}}^{\mathrm{tot}} + 2k_{\mathrm{D}}^t + 2k_{\mathrm{D}}^t({k_{\mathrm{R}}^t}^2 + 1) + 2k_{\mathrm{D}}^t(k_{\mathrm{D}}^{\mathrm{tot}} - k_{\mathrm{D}}^t)^2 - 2{k_{\mathrm{D}}^t}^2(k_{\mathrm{D}}^{\mathrm{tot}} - k_{\mathrm{D}}^t). \tag{64}$$

The expression $\frac{\partial\phi^\infty}{\partial k_{\mathrm{D}}^t}$ can be obtained similar to (48) by changing k_{R}^t to k_{D}^t. Then by substituting (49)–(57) and (63), (64) into $\frac{\partial\phi^\infty}{\partial k_{\mathrm{D}}^t}$, and after manipulations, we obtain

$$\frac{\partial\phi^\infty}{\partial k_{\mathrm{D}}^t} = -\frac{2\left(2k_{\mathrm{R}}^2k_{\mathrm{D}}^t - 2{k_{\mathrm{D}}^t}^2k_{\mathrm{D}}^{\mathrm{tot}} + 2k_{\mathrm{D}}^t{k_{\mathrm{D}}^{\mathrm{tot}}}^2 + 3k_{\mathrm{D}}^t - 2k_{\mathrm{D}}^{\mathrm{tot}}\right)}{\left(2k_{\mathrm{R}}^2 + 3{k_{\mathrm{D}}^t}^2 - 4k_{\mathrm{D}}^tk_{\mathrm{D}}^{\mathrm{tot}} + 2{k_{\mathrm{D}}^{\mathrm{tot}}}^2\right)^2}. \tag{65}$$

It is straightforward to see that (65) is a concave function of k_{D}^t in the feasible set and the single solution to $\frac{\partial\phi^\infty}{\partial k_{\mathrm{D}}^t} = 0$ is simply calculated.

APPENDIX C

We can write

$$\frac{\partial \phi^{\infty}}{\partial k_{\mathrm{R}}^{r}} = \frac{\partial \phi^{\infty}}{\partial \tau_2}\frac{\partial \tau_2}{\partial k_{\mathrm{R}}^{r}} + \frac{\partial \phi^{\infty}}{\partial \xi_1}\frac{\partial \xi_1}{\partial k_{\mathrm{R}}^{r}}. \tag{66}$$

Using (45) yields

$$\frac{\partial \phi^{\infty}}{\partial \tau_2} = -\frac{\xi_1\Big[\left(2\left(\tau_2{+}2\right)\xi_1{-}{\tau_2}^2\right)\sqrt{\xi_1(1{+}\tau_2)}{+}2\xi_1(\tau_2(\xi_1{+}1{-}\tau_2){+}\xi_1{+}1)\Big]}{2{\tau_2}^2\left(\sqrt{\xi_1}\sqrt{1{+}\tau_2}{+}\,1\right)^2\left(\xi_1{+}\sqrt{\xi_1}\sqrt{1{+}\tau_2}\right)^2}, \tag{67}$$

$$\frac{\partial \phi^{\infty}}{\partial \xi_1} = \frac{(1+\tau_2)\left[\left(\tau_2+2\xi_1\right)\sqrt{\xi_1(1+\tau_2)}+2\left(1+\tau_2\right)\xi_1\right]}{2\tau_2\left(\sqrt{\xi_1}\sqrt{1+\tau_2}+1\right)^2\left(\xi_1+\sqrt{\xi_1}\sqrt{1+\tau_2}\right)^2}. \tag{68}$$

Considering $k_{\mathrm{R}}^{t} = k_{\mathrm{R}}^{\mathrm{tot}} - k_{\mathrm{R}}^{r}$, one can obtain

$$\frac{\partial \tau_2}{\partial k_{\mathrm{R}}^{r}} = 4{k_{\mathrm{R}}^{r}}^{3} - 6{k_{\mathrm{R}}^{r}}^{2}k_{\mathrm{R}}^{\mathrm{tot}} + (2{k_{\mathrm{D}}^{r}}^{2} + 2{k_{\mathrm{R}}^{\mathrm{tot}}}^{2} + 4)k_{\mathrm{R}}^{r} - 2k_{\mathrm{R}}^{\mathrm{tot}}, \tag{69}$$

$$\frac{\partial \xi_1}{\partial k_{\mathrm{R}}^{r}} = 2k_{\mathrm{R}}^{r}. \tag{70}$$

By substituting (67)–(70) into (66) and solving $\frac{\partial \phi^{\infty}}{\partial k_{\mathrm{R}}^{r}} = 0$ yields $k_{\mathrm{R}}^{r} = \frac{k_{\mathrm{R}}^{\mathrm{tot}}}{2}$.

Acknowledgements

The authors would like to thank Prof. Lajos Hanzo for helpful comments to improve the paper.

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys and Tutorials*, vol. 16, no. 3, pp. 3062-3080, Feb. 2014.

[2] X. Chen, D. W. K. Ng, W. Gerstacker, and H-H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Commun. Surveys Tuts.*, doi: 10.1109/COMST.2016.2633387.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[4] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Sig. Proc. Mag.*, vol. 30, no. 1, pp. 40-46, Jan. 2013.

[5] E. G. Larsson, F. Tufvesson, O. Edfors, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186-195 , Feb. 2014.

[6] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of BS antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590-3600, Nov. 2010.

[7] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21-27, Jun. 2015.

[8] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," *in Proc. IEEE Globecom*, New Orleans, LA, Dec. 2008, pp. 15.

[9] M. R. A. Khandaker and K-K Wong, "Masked Beamforming in the Presence of Energy-Harvesting Eavesdroppers," *IEEE Trans. Inf. Forens. Sec.*, vol. 10, no. 1, pp. 40-54, Jan. 2015.

[10] M. R. A. Khandaker and K.-K. Wong, "Robust secrecy beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 10-13, Feb. 2015.

[11] Y. Liu, A. P. Petropulu, and H. V. Poor, "Joint decode-and-forward and jamming for wireless physical layer security with destination assiatance," in *Proc. Asilomar Conference on Signals, Systems and Computer (ASILOMAR11),* Pacific Grove, USA, Nov. 2011.

[12] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE J. Sel. Areas Commun.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[13] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536-2550, May 2013.

[14] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801-3807, Oct. 2012.

[15] W. Wang, K. C. Teh, and K. H. Li, "Secure Cooperative AF Relaying Networks with Untrustworthy Relay Nodes," in *IEEE Globecom*, Washington, DC. 2016, pp. 1-6.

[16] A. Mabrouk, K. Tourki, and N. Hamdi, "Secure cooperative untrusted-relay network with outdated CSI," in *IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, 2016, pp. 90-95.

[17] A. Kuhestani, A. Mohammadi, and M. Noori, "Optimal Power Allocation to Improve Secrecy Performance of Non-Regenerative Cooperative Systems Using an Untrusted Relay," *IET Commun.*, vol. 10, no. 8, pp. 962-968, May 2016.

[18] A. Kuhestani, A. Mohammadi, and P. L. Yeoh, "Optimal Power Allocation and Secrecy Sum Rate in Two-Way Untrusted Relaying," Submitted to *IEEE Trans. Veh. Technol.*, Apr. 2017.

[19] L. Lv, J. Chen, L. Yang, and Y. Kuo, "Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation," *IET Commun.*, vol. 11, no. 3, pp. 393-399, Jul. 2017.

[20] T. Mekkawy, R. Yao, F. Xu, and L. Wang, "Optimal power allocation for achievable secrecy rate in an untrusted relay network with bounded channel estimation error," in *26th Wireless and Optical Communication Conference (WOCC)*, Newark, NJ, USA, 2017, pp. 1-5.

[21] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-Aware Relaying Scheme for Cooperative Networks with Untrusted Relay Nodes," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 463-466, Sep. 2014.

[22] T. Schenk, *RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation*, Springer, 2008.

[23] C. Studer, M. Wenk, and A. Burg, "MIMO transmission with residual transmit-RF impairments," in *Proc. ITG/IEEE Workshop on Smart Antennas*, Feb. 2010.

[24] E. Bjornson, A. Papadogiannis, M. Matthaiou, and M. Debbah, "On the impact of transceiver impairments on AF relaying," in *Proc. 2013 IEEE Int. Conf. Acoustics, Speech, Signal Process.*

[25] A. A. A. Boulogeorgos, D. S. Karas, and G. K. Karagiannidis, "How Much Does I/Q Imbalance Affect Secrecy Capacity?," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1305-1308, July 2016.

[26] J. Zhu, R. Schober, and V. K. Bhargava, "Physical Layer Security for Massive MIMO Systems Impaired by Phase Noise," *IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications*, pp. 1-5, Jul. 2016.

[27] J. Zhu, R. Schober and V. K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245-2261, Mar. 2016.

[28] J. Chen, X. Chen, W. H. Gerstacker and D. W. K. Ng, "Resource Allocation for a Massive MIMO Relay Aided Secure Communication," *IEEE Trans. Inf. Forens. Sec.*, vol. 11, no. 8, pp. 1700-1711, Aug. 2016

[29] J. Chen, H. Chen, H. Zhang and F. Zhao, "Spectral-Energy Efficiency Tradeoff in Relay-Aided Massive MIMO Cellular Networks With Pilot Contamination.," *IEEE Access*, vol. 4, no. , pp. 5234-5242, Sept. 2016.

[30] L. Wang, Y. Cai, Y. Zou, W. Yang and L. Hanzo, "Joint Relay and Jammer Selection Improves the Physical Layer Security in the Face of CSI Feedback Delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259-6274, Aug. 2016.

[31] B. E. Priyanto, T. B. Sorensen, O. K. Jensen, T. Larsem, T. Kolding, and P. Mogensen, "Assessing and modelling the effect of RF impairments on UTRA LTE uplink performance," in *Proc. 2007 IEEE Vehic. Techn. Conf. Fall*, pp. 12131217.

[32] K. S. Ahn and R. W. Heath, "Performance analysis of maximum ratio combining with imperfect channel estimation in the presence of cochannel interferences," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 1080-1085, Mar. 2009.

[33] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.

[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York: Academic, 2007.