IECO International Journal Of Industrial Electronics Control and Optimization
Print ISSN: 3517-2645
Online ISSN: 3568-2645
Homepage: https://ieco.usb.ac.ir/

Energy efficient power allocation by Imperfect Hardware Analysis in Untrusted Relaying

Mohammad Ragheb[1] | **Ali Kuhestani**[2] | **Mohammad Reza Keshavarzi**[3]

[1] Qom University of Technology, Faculty of Electrical and Computer Engineering, Qom, Iran,
[2] Faculty member of Qom University of Technology, Qom, Iran,
[3] ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran
Corresponding authors' email: mohamad_ragheb@yahoo.com and kuhestani@qut.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: *************
Received in revised form: *************
Accepted: *************
Published online: ************

Keywords:
Energy efficient communications, Power allocation, Untrusted Relaying, Hardware impairments.

ABSTRACT

In this study, the authors investigate the impact of residual additive hardware impairments (HWIs) on the energy efficiency of a cooperative secure communication system. Within the framework of physical layer security and from the viewpoint of green communications, an energy efficient (EE) optimization technique is proposed for an amplify-and-forward (AF) relay network under the assumption that HWIs are present at the relay. Specifically, the authors derive the optimal transmit power at the base station (BS) to minimize the relay's transmit power. The system employs the destination-based cooperative jamming (DBCJ) scheme, in which the BS securely transmits information to the user equipment (UE) via an untrusted relay.
First, the case where HWIs exist only at the relay's receiving side is considered. Assuming a fixed power for the CJ signal, a closed-form expression for the optimal transmit power is obtained, showing that it is inversely proportional to the first-hop channel gain. Subsequently, when HWIs are present only on the transmitting side of the relay, a similar closed-form expression is derived under the same CJ-power assumption. These results effectively characterize the influence of residual HWIs on system performance and demonstrate that higher first-hop channel quality leads to a lower required transmit power, thereby improving overall energy efficiency. Moreover, for example, when the BS transmit power is approximately 25 dBm, if the relay suffers from HWIs on its transmitting side, about 0.5 dBm higher relay power consumption is required compared to the ideal relay case in order to ensure reliable communication. Furthermore, HWIs at the relay transmitter have a less significant impact compared to those at the relay receiver. This result indicates that, when purchasing a relay, greater cost should be allocated to the RF receiver section than to the transmitter section.

NOMENCLATURE

$\boldsymbol{h}_{sr}$	Complex Gaussian channel from source to relay	R_s	Instantaneous secrecy rate of one-way relaying network
$\boldsymbol{h}_{rd}$	Complex Gaussian channel from relay to destination	$\hat{R}_s$	A minimum required target rate
N_s	Number of antennas at the source	P_s	Transmit power of source
N_d	Number of antennas at the destination	P_d	Transmit power of destination
η_R^r	Residual hardware impairment (HWI) in the relay's receiver	μ_{sr}	Channel gain related to the distance-dependent path loss for BS antenna
η_R^t	Residual HWI in the relay's transmitter	μ_{rd}	Channel gain related to the distance-dependent path loss for UE antenna
κ_R^r	HWI level at the relay's receiver	$\lvert W^*\rvert$	Optimal amplification weight
κ_R^t	HWI level at the relay's transmitter	$\Phi(P_s, P_d$	Relay power transmission
		$P_{r,T}$	Relay average power transmission

I. Introduction

The relaying technique is beneficial for enhancing reliability, extending communication coverage, and improving energy efficiency [1]. It plays a particularly important role in communications highly susceptible to blockage, by enabling link closing and increasing coverage. In recent years, relaying has also been widely adopted to strengthen physical-layer security (PLS) in wireless systems. However, a key challenges is the limited battery life of miniature wireless relay nodes and the need to protect the information forwarded by relay nodes from source to destination. These issues are especially critical for Internet-of-Things (IoT) applications with mobile connectivity beyond fifth-generation B5G/6G mobile communications for heterogeneous network deployments. To this end, Dutriez *et al.* [2] proposed an energy-efficient (EE) relay selection method in which relays are chosen so as to maximize the overall network lifetime, while maintaining a certain level of Quality of Service (QoS). Considering that the system model is deployed in a dynamic and unknown environment, they employed a deep reinforcement learning technique aimed at optimizing network relay selection, maximizing the residual energy levels of devices, and ensuring fair and high data rates.

Since wireless communication is subject to eavesdropping attacks, information security needs special attention. To achieve this vital goal, in recent years, PLS techniques have been considered as efficient and practical solutions in various communication systems [3]. Recently, several studies have examined the impact of node cooperation on the achievable secrecy rate [4]. This strategy, known as cooperative jamming (CJ), reduces the eavesdropper's received signal-to-noise-ratio (SNR). An approach in which distributed Gaussian artificial noise is injected into the null space of the intended receiver to ensure communication secrecy was investigated in [5]. While most recent works focus on scenarios where relays are trusted and can act as friendly helpers to counter external eavesdroppers, in some applications, the relay may be an untrusted entity [5], [6], [7]; thus, the transmitted messages must be kept hidden from it. For example, in a public network, an untrusted relay might be used without having equivalent security clearance. In such networks, the relays required for connectivity may be untrusted. To prevent the untrusted amplify-and-forward (AF) relay from eavesdropping, the authors in [4] injects a known artificial noise signal as destination-assisted cooperative jamming and derived a closed-form expression for maximizing the ergodic secrecy rate over Rayleigh fading relay channels. Additionally, Dianxia *et al.* [8] considered a scenario in which the source intends to send a message to the destination via a relaying scheme — due to long communication distance and limited transmission power — in the presence of multiple eavesdroppers (Eves). They proposed two types of joint relay and jammer selection methods under the assumption of both perfect channel state information (CSI) and average CSI of the eavesdroppers.

The first proposed strategy to achieve a positive secrecy rate in untrusted relaying is destination-based CJ (DBCJ), in which CJ is performed at the destination for the source-to-destination communication [5], [6], [7]. The destination then completely cancels the jamming signal via self-interference cancellation. Recently, some papers have analyzed the performance of the DBCJ technique for untrusted relay networks [5], [6], [7].

Under the time switching relaying protocol, Shi *et al.* [9] proposed a PLS transmission scheme based on the CJ and showed that increasing the transmitting power of untrusted relay node is beneficial to improve the connection reliability of the system. PLS based on non-orthogonal multiple access (NOMA) and CJ is considered in a one-way AF relay network with an untrusted relay [10]. In such a scenario, Yu *et al.* [10] demonstrated that their proposed PLS scheme achieves a higher secrecy rate than a secure beamformed transmission based on NOMA and artificial noise. Quantum key distribution (QKD) has demonstrated a great potential to provide future-proofed security, especially for 5G and B5G. In this regard, Cao *et al.* [11] studied the hybrid trusted/untrusted relay based QKD deployment over optical backbone networks and focus on cost optimization during the deployment phase.

Green communication is playing a more important role in future wireless communications [12]. Furthermore, wireless relay nodes need to save energy when operating for longer durations away from centralized power supplies. From the system's perspective, energy-efficient communications are sometimes considered as an important topic for future networks. For example, in a wireless network with limited battery capacity, the network's lifetime depends on the power consumed by the nodes. Therefore, the problem of minimizing the total transmit power or relay power, subject to predefined quality-of-service constraints, is of concern. Motivated by this issue, some studies have examined energy efficiency in secure wireless communication systems [13], [7], [14]. For an energy harvesting relay network, an optimal secure transmission scheme in the case of DBCJ technique is applied by the authors of [14] to protect the confidential information from relay's jamming and eavesdropping. Moreover, Zhao *et al.* [13] used DBCJ to prevent the leakage of information during the offloading process. Under the condition of time delay and energy consumption, they jointly optimized the transmission power allocated to untrusted relay, central processing unit frequency and offloading time to maximize the security energy efficiency of the user.

One of the essential considerations in the design of wireless systems is the presence of hardware impairments (HWIs) such as I/Q imbalance, oscillator phase noise, high power amplifier nonlinearities, and quantization errors [6], [15], [16], [17]. The severity of the impairments also depend\ on the quality of the hardware used in the RF transceivers.

Non-ideal hardware in practical applications further impacts energy efficiency, making research into high-energy-efficiency MIMO structures [12]. In this regard, a highly effective hybrid precoding strategy has been developed in [12] that incorporates the consequences of non-ideal hardware characteristics. Although HWIs can be mitigated through analog and digital signal processing methods, due to the randomness of various sources of HWIs, they cannot be completely eliminated. This is because, for example, inaccurate models are used to describe the behavior of HWIs, incomplete parameters arise for estimation errors due to thermal noise, and discontinuous compensation algorithms with limited capabilities are adopted. The residual HWIs in the transceiver can be modeled as a combination of multiplicative phase noise and additive distortion noise at both the transmitter and the receiver.

Recently, the authors of [18] have proposed the STEALTH (Space-time encryption via constellation hiding) scheme to enhance PLS in MIMO two-way untrusted relay systems by exploiting space–time constellation hiding. The RIS-assisted two-way relay framework studied in [19], where secrecy energy efficiency is enhanced through the joint iterative optimization of RIS phase shifts and beamforming under ideal hardware assumptions. The integration of Edge Computing and AI in frameworks like the 5G-R system proposed in [20] represents a significant step toward robust high-mobility connectivity. Nevertheless, the sustainability of these advanced architectures depends on energy-aware and secure transmission protocols.

In this paper, our analysis focuses on the effect of the residual additive HWIs as stated in most of the literature [6], [22]. In this paper, from the perspective of green communications within the PLS framework, we propose an EE technique for an AF relay network under the assumption of HWIs at the relay and obtain the optimal signal power. The considered system employs the DBCJ technique, whereby the base station (BS) securely transmits its signal to the user equipment (UE) through an untrusted relay. First, we assume that the HWI exists only in the receiving side of the relay. As demonstrated by Kazemi *et al.* [22], such impairment has a dominant effect compared to other HWI in their studied system with the decode-and-forward (DF) relay selection strategy. Under the assumption of a fixed power for the transmitted CJ, we derive a closed-form expression for the optimal signal power that minimizes the relay's transmit power. It is observed that this optimal power is inversely proportional to the channel gain of the first hop. Subsequently, we assume that the HWI exists only in the transmitting side of the relay. For this case as well, under the same assumption of fixed CJ power, a closed-form expression for the optimal signal transmit power, aimed at minimizing the relay's transmit power, is derived.

Although the approach used in [18] achieves strong secrecy without relying on additional jamming power and demonstrates accurate BER analysis, it does not explicitly address energy-efficiency optimization nor consider the impact of HWIs, which are critical factors in practical IoT-oriented relay networks. Different from [19], this work focuses on a DBCJ scheme in untrusted AF relaying networks while explicitly accounting for residual HWIs. By adopting practical EVM-based HWI models at the relay transceiver, we derive closed-form expressions for the optimal transmit power that minimize the relay power consumption under a target secrecy rate constraint. Unlike RIS-based approaches that rely on alternating optimization with high computational and signaling overhead, the proposed solution provides low-complexity analytical insights, revealing the fundamental coupling between HWIs, cooperative jamming, and energy efficiency in practical untrusted relay systems. Unlike [20], which focuses on AI-based connectivity management, this paper investigates the EE design of a DBCJ scheme.

The main contributions of this paper compared to some related papers are summarized as follows:

- Inspired by [6], [15], [22], we first present the generalized system model for relay HWIs in the receiving side 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. Next we model the relay HWI in the transmitting side. Based on this, we calculate the received instantaneous SNDR at the relay and destination.
- Unlike [15], where the destination is single-antenna, in our system model the destination is multi-antenna. Moreover, as the respected reviewer pointed out, our objective is to minimize the relay transmit power while satisfying a minimum secrecy rate, whereas the authors of [15] pursued optimal power allocation with the aim of maximizing the instantaneous secrecy rate.
- We investigated the impact of relay HWIs on the system energy efficiency in two scenarios: HWI at the relay receiver and HWI at the relay transmitter, and the results show that HWIs at the relay transmitter have a smaller impact compared to those at the receiver. This issue has not been investigated in [15]. Moreover, our findings show that, for example, for a BS transmit power of about 25 dBm, when the relay suffers from transmitter-side HWI, the relay requires approximately 0.5 dBm higher transmit power compared to the ideal relay case studied in [7] in order to achieve secure transmission.
- In each of them, we formulate the optimal power allocation (OPA) of the source that minimizes the relay power minimization of untrusted relaying. Accordingly, novel closed-form solutions are derived for the exact OPA.
- In this work we have considered HWIs at the relay node, which is modeled as a low-cost element. However, as evident from the analytical derivations, this consideration

leads to more complicated expressions. Moreover, in order to observe the impact of HWIs on the relay power expression, we do not assume the high-SINR regime, which further increases the mathematical complexity. This highlights the broader applicability and greater generality of our work compared to [7]. Consequently, instead of the simple derivative-based approach adopted in [7], we are required to perform more involved differentiation and to employ software tools such as MATLAB and Maple to solve the resulting optimization problem. Accordingly, the trends observed in [7] do not appear in our simulation results.

In the rest of this article, the introduced methodology and modeling will be given in Section II. Section III presents energy-efficiency criterion and discussions. Section IV presents numerical results and discussion. Finally, the conclusion is drawn in Section V.

II. System model and problem definition

We consider a two-hop DBCJ wireless network which consists of a multiple antenna source and a multiple antenna destination with N_s and N_d antennas, respectively and a single antenna, untrusted AF relay as seen in Fig. 1. We also assume that the channels satisfy the reciprocity theorem [6]. The transmit power of source and destination are represented by P_s and P_d, respectively. Each node operates in a half-duplex mode and there is no direct link between source and destination. In the proposed protocol, during the first phase, while the source transmits the information signal, the destination transmits the jamming. During the second phase, the relay sends the scaled version of the received signals to destination. The complex Gaussian channel from source to relay and relay to destination are denoted by $\boldsymbol{h}_{sr}\sim\mathcal{CN}(0_{N_s\times 1},\mu_{sr}\boldsymbol{I}_{N_s})$ and $\boldsymbol{h}_{rd}\sim\mathcal{CN}(0_{N_d\times 1},\mu_{rd}\boldsymbol{I}_{N_d})$, respectively, where μ_{sr} and μ_{rd} are the channel gains related to the distance-dependent path loss for each antenna branch. The additive white noise, n_m $(m\in\{r,d\})$ at each receiver is represented by a zero-mean complex Gaussian variable with variance σ_n^2 which is assumed to be known at the receiving nodes. To model the statistical behavior of the residual HWIs, we adopt the model presented in [23], which has also been widely employed in several related studies, including [6], [15], [21]. Accordingly, denoting the residual HWI in the relay's receiver and transmitter are denoted by η_R^r and η_R^t, respectively. The impairments at R are modeled as $\eta_R^r\sim\mathcal{CN}\left(0,\ {\kappa_R^r}^2(P_s\|h_{sr}\|^2+P_d\|h_{rd}\|^2)\right)$, $\eta_R^t\sim\mathcal{CN}\left(0, P_s{\kappa_R^t}^2\right)$, where $\kappa_R^r>0$ and $\kappa_R^t>0$ characterize the HWI levels at the relay's receiver and transmitter, respectively. These parameters are defined as the error vector magnitudes (EVMs). EVM is defined as the ratio of the average distortion magnitude to the average signal magnitude and determines the quality of RF transceivers. Since the EVM captures the combined effects of various HWIs as well as the associated compensation algorithms, it can be directly measured in practical transceiver implementations [6], [23]. 3GPP LTE specifies EVM requirements at frequencies below 6 kHz in the range of [0.08, 0.175] [24] which can be reached to 0.3 for higher frequencies such as millimeter wave and THz [15], [25].

For simplicity of our analysis, we first consider the impairments in the relay's receiver and then consider the HWI in the relay's transmitter.

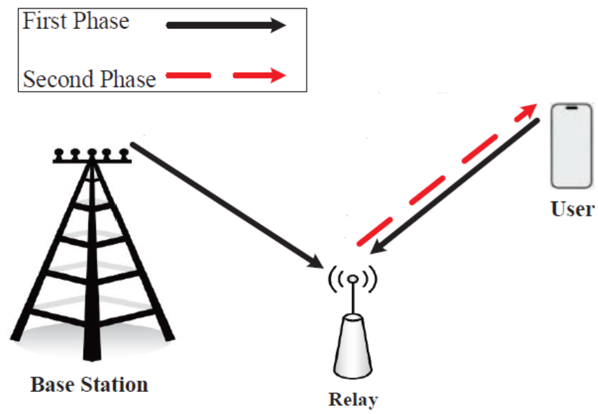

Fig. 1. One-way relaying between a multiple antenna BS and a multiple antenna UE via an untrusted AF relay under the presence of transceiver impairments for the relay.

In the first phase, the source transmits its message x_s, and simultaneously, the destination emits the jamming signal x_d. We consider $\mathbb{E}\{|x_s|^2=1\}$ and $\mathbb{E}\{|x_d|^2=1\}$. Considering the use of multiple antennas, we employ maximum ratio transmission (MRT) at the BS in the first phase and maximum ratio combining (MRC) at the UE in the second phase. We assume that the BS and UE have full knowledge of the channel gains from the BS to the relay and from the relay to the UE, respectively, in order to perform MRT and MRC. This assumption is applicable for slow-fading channels where the block time of a message exchange remains constant.

As a result, the actual received signal at the relay node can be expressed as

$$y_R=\sqrt{P_s}\boldsymbol{h}_{sr}\boldsymbol{W}_S x_s+\sqrt{P_d}\boldsymbol{h}_{dr}\boldsymbol{W}_d x_d+\eta_R^r+n_R. \quad (1)$$

***Remark 1**:* Each node in the proposed system model operates in a half-duplex mode. Considering the time-division duplexing (TDD) operation, the source acquires the downlink CSI through uplink training. Since all the channels satisfy the reciprocity theorem, we replace h_{dr} with h_{rd}. The estimated CSI is then employed to construct the MRT precoding matrix, which offers low implementation complexity.

In the second phase of transmission, the relay amplifies its received signal by a positive factor w and transmits its message as

$$x_R=wy_R. \quad (2)$$

The relay forwards x_R to the destination. Hence, the useful received signal after cancelling self-interference, i.e. x_d, at the destination is

$$\boldsymbol{y}_D = \underbrace{\sqrt{P_s} w \|\boldsymbol{h}_{sr}\| \boldsymbol{h}_{rd} x_s}_{Information\ Signal} + \underbrace{w \boldsymbol{h}_{rd} n_r + \boldsymbol{n}_D}_{AWGN\ Noise} + \underbrace{w \eta_{R,k}^{r} \boldsymbol{h}_{rd}}_{Distortion\ Noise} . \quad (3)$$

We note that, MRT transmits the weighting vectors at the BS as $\boldsymbol{W}_S = \frac{\boldsymbol{h}_{sr}^H}{\|\boldsymbol{h}_{sr}\|}$, and MRC received the weighting vectors at the UE as $\boldsymbol{W}_d = \frac{\boldsymbol{h}_{rd}^H}{\|\boldsymbol{h}_{rd}\|}$.

By invoking (1), the achievable signal-to-interference-plus-noise ratio (SINR) at the relay is expressed as

$$\gamma_R = \frac{\lambda_s P_s}{\lambda_d P_d + {K_R^r}^2(\lambda_s P_s + \lambda_d P_d) + \sigma_n^2}, \quad (4)$$

where $\lambda_s = \|\boldsymbol{h}_{sr}\|^2$ and $\lambda_d = \|\boldsymbol{h}_{rd}\|^2$.

Moreover, by invoking (3), the SINR at the destination can be obtained as

$$\gamma_D = \frac{\lambda_w \lambda_s \lambda_d P_s}{\lambda_w {K_R^r}^2 \lambda_d(\lambda_s P_s + \lambda_d P_d) + \lambda_w \lambda_d \sigma_n^2 + \sigma_n^2}, \quad (5)$$

where $\lambda_w = |w|^2$.

It is worth noting that the multi-antenna receiver employs MRC to process the received signal. Under the multi-antenna reception assumption, and considering the independence between the noise and the combining vector, the noise power after combining can be approximated as $|\boldsymbol{w}_d \boldsymbol{n}_d|^2 \approx E[|\boldsymbol{w}_d \boldsymbol{n}_d|^2] = E[|\boldsymbol{w}_d|^2] E[|\boldsymbol{n}_d|^2]$. Since the combining vector is normalized, i.e., $E[|\boldsymbol{w}_d|^2] = 1$, and the additive noise satisfies $E[|\boldsymbol{n}_d|^2] = \sigma_n^2$, it follows that $|\boldsymbol{w}_d \boldsymbol{n}_d|^2 \approx \sigma_n^2$.

III. Energy-efficient (EE) criterion

In this section, we try to find the relay weighting coefficient such that while satisfying a minimum required target rate $\hat{R}_s$, the relay power P_r is minimized. In the first stage, we assume that only the relay's receiver suffer from HWIs and then in the next stage we assume that only the relay's transmitter suffer from HWIs.

A. *Relay power minimization with relay's receiver HWI*

In this scenario, while the relay's power is limited the source and destination powers can be fully supported. Some communication links in IoT applications are in this category [26]. We note furthermore that in modern communication architectures, especially in IoT networks, the assumption of limited relay power but higher power at the source and destination is not only realistic but also a principle of green network design. This limitation has led to the development of areas such as: design of smart relays with energy harvesting (EH Relays), Deep Q-Network (DQN) algorithms for dynamic power allocation energy and efficiency metrics modeling. To maximize the network lifetime, the relay power minimization should be paid great attention. Here, we consider the relay power minimization problem when the source power $P_s > 0$ and the destination noise power $P_d > 0$ are given. For simplicity and without losing of generality, we assume that the power of P_d is constant. Therefore, the minimization problem i.e., the relay power P_r minimization subject to a minimum required target rate $\hat{R}_s$ can be formulated as

$$\begin{aligned} &\min_{\substack{P_s,\, \lambda_w \\ s.t.\ \ R_s \geq \hat{R}_s,\, P_s > 0 \\ ,\, P_d > 0,\ \ \lambda_w > 0}} \quad P_r . \\ &P_r = \lambda_w\big(\lambda_s P_s + \lambda_s P_s {\kappa_R^r}^2 + \lambda_d P_d + \lambda_d P_d {\kappa_R^r}^2 + \sigma_n^2\big) \end{aligned} \quad (6)$$

Due to the definition of instantaneous secrecy rate of one-way relaying network [27], which is defined as

$$R_s = (1/2)[\log_2(1+\gamma_D)/(1+\gamma_R)]^+, \quad (7)$$

where $[x]^+ = \max(x, 0)$. If we assume $P_s = P_d = 0$, and substitute these values into Eq. (7), we obtain $R_s = 0$. However, since the goal is to allocate a certain transmit power to the receiver and an optimal transmit power to the transmitter, a non-negative secrecy rate becomes achievable. In this case, the $[.]^+$ operator can be removed, and the instantaneous secrecy rate can again be written and reformulated as $R_s = [R_s]^+$. The optimal solution of (6) is obtained when the first inequality constraint is met, i.e. $R_s = \hat{R}_s$.

Remark 2*:* If the channel conditions are very poor (infeasible state), naturally the constraint $R_s = \hat{R}_s$ cannot be satisfied. In other words, $[x]^+ = max(x, 0) = 0$; therefore, in this case the network is inactive and the relay is turned off, meaning that no transmission takes place. In such infeasible cases, the system naturally operates in a silence (outage) mode with zero transmission. This modeling approach is well aligned with recent studies on physical layer security such as [18]. In contrast, when the channel conditions are favorable (feasible state), $R_s = \hat{R}_s > 0$, and thus there is no need to apply the operation $[x]^+ = max(x, 0)$; in fact, $[x]^+ = x$.

It should be noted that the corresponding objective function is independent of the phase of $|w| = \sqrt{\lambda_w}$; therefore, no phase compensation is needed at the relay. By invoking (4) and (5) into (7) and after solving the equation $R_s = \hat{R}_s$ respect to λ_w, the optimal value of λ_w i.e. λ_W^* is reached as

$$\begin{aligned} \lambda_w^* &= \frac{\sigma_n^2}{\lambda_d}\left[\frac{U_1}{P_s\lambda_s - \left((\lambda_s P_s + \lambda_d P_d){\kappa_R^r}^2 + \sigma_n^2\right)U_1}\right], \\ U_1 &= \left(1 + \frac{\lambda_s P_s}{\lambda_d P_d + {\kappa_R^r}^2(\lambda_s P_s + \lambda_d P_d) + \sigma_n^2}\right)K - 1 \end{aligned} \quad (8)$$

where $K = 2^{2\hat{R}_s}$. Since, we use an approximation for λ_W^* we omitted writing the exact value here. Substituting (8) into

(6), the optimization problem is reformulated by the following unconstrained problem

$$\min_{P_s>0} \Phi(P_s, P_d)|_{P_d=cnt}, \quad (9)$$

where

$$\Phi(P_s) = \lambda_W^*((\lambda_s P_s + \lambda_d P_d)(1+\kappa_R^{r\,2}) + \sigma_n^2), \quad (10)$$

and the feasible set is $P_s > 0$ and $P_d = cte$. Here, *cnt* denotes an assumed constant value. As can be observed from the expression of (10), minimizing the relay transmit power, $\Phi(P_s)$ leads to the determination of the BS transmit power, P_s^* that corresponds to the minimum achievable relay power under the imposed secrecy constraint. Therefore, by appropriately adjusting the BS transmit power, the minimum achievable relay transmit power can be attained. From an intuitive standpoint, if the relay transmit power is chosen to be excessively small, the secrecy constraint $R_s \geq \hat{R}_s$ cannot be satisfied. Since the secrecy rate R_s is jointly determined by the transmit powers of the BS and the UE, an appropriate adjustment of these powers enables the system to satisfy $R_s = \hat{R}_s$ while simultaneously achieving the minimum relay transmit power. For analytical tractability, the UE transmit power is assumed to be fixed in this work.

We start finding the optimal solution for the optimization problem: namely P_s^*, by proving that $\Phi(P_s)$ is a convex or quasi-convex function of P_s.

Theorem 1*:* $\Phi(P_s)$ is a convex function of P_s.

Proof: By taking two times partial derivative from $\Phi(P_s)$ with respect to P_s, one can arrive at, $\frac{\partial^2\Phi(P_s)}{\partial {P_s}^2}$ is positive in the feasible set. Therefore, $\Phi(P_s)$ is a convex function of P_s in the feasible set. We mention that, due to long derivative equation and space limitations, the proof is omitted here. For further clarification, it should be noted that, the authors of [7] using an AF relay transmission model with *ideal hardware*, proved the convexity of Φ. Now, by performing a few factorization steps in (10), $\Phi(P_s)$ can be rearranged as a function of $(1+\kappa_R^{r\,2})$. Intuitively, it can be seen that $\Phi(P_s)$ in our system model merely adds a very small value of $\kappa_R^{r\,2}$ to the constant value of 1 respect to the similar Φ in [7]. In this case, it can be inferred that no change should occur in the convexity of our new Φ.

Regarding ***Remark 1*** and ***Theorem 1***, and considering that κ_R^r is a small number, the optimal point of (9) i.e., the signal power is found by solving $\frac{d\Phi(P_s)}{dP_s}|_{P_d=cnt} = 0$, and approximated by

$$P_s^* = -\frac{1}{\lambda_s K} \times \frac{\left(K(K-1)\sigma_n^2 + K\kappa_R^{r\,2} P_d + S_1\right)(\lambda_d P_d + \sigma_n^2)}{-\lambda_d P_d\left(1+\kappa_R^{r\,2}\right) + (K-1)\sigma_n^2}. \quad (11)$$

$$S_1 \triangleq \sqrt{K\lambda_d P_d (K-1)\left(\lambda_d P_d\left(1+2\kappa_R^{r\,2}\right)+\sigma_n^2\right)}$$

It should be noted that, due to network dynamics, the optimal BS transmit power varies for different channel realizations. Moreover, as can be observed from Eq. (4), if the BS–relay channel gain is large, the received power at the relay increases; consequently, the relay can deliver the signal to the destination with a lower gain. Therefore, a dependency between the relay power gain and the channel gains exists.

We further explain that depending on the channel conditions, R_s may not be achievable and as a result, positive P_s and w may not be found. In this situation, the transmitter keeps silence and we have no transmission.

In large scale antenna (LSA) regime at the source and destination, we can approximate the channel gains as

$$\lambda_s = \|\boldsymbol{h}_{sr}\|^2 \overset{(a)}{\approx} N_s\mu_{sr}, \; \lambda_d = \|\boldsymbol{h}_{rd}\|^2 \overset{(b)}{\approx} N_d\mu_{rd}, \quad (12)$$

where *(a) and (b)* follows from the law of large numbers [28] due to large N_s and N_d. Moreover, μ_{sr} and μ_{rd} are channel gains related to the distance-dependent path loss for BS and UE antennas respectively. By applying (12) in (11), P_s^* can be rewritten as

$$P_s^* = -\frac{1}{N_s\mu_{sr}K} \times \frac{K(K-1)\sigma_n^2 + KK_R^{r\,2}N_d\mu_{rd}P_d + S_2}{-N_d\mu_{rd}P_d\left(1+K_R^{r\,2}\right)+(K-1)\sigma_n^2} \times (N_d\mu_{rd}P_d + \sigma_n^2). \quad (13)$$

$$S_2 \triangleq \sqrt{KN_d\mu_{rd}P_d(K-1)\left(N_d\mu_{rd}P_d\left(1+2\kappa_R^{r\,2}\right)+\sigma_n^2\right)}$$

The optimal amplification weight is obtained after replacing (12) at (8) as

$$|W^*| = \sqrt{\frac{\sigma_n^2}{N_d\mu_{rd}}} \times \sqrt{\frac{U_2}{N_s\mu_{sr}P_s - \left(\kappa_R^{r\,2}(N_s\mu_{sr}P_s + N_d\mu_{rd}P_d) + \sigma_n^2\right)U_2}}. \quad (14)$$

$$U_2 \triangleq (1 + \frac{N_s\mu_{sr}P_s}{N_d\mu_{rd}P_d + \kappa_R^{r\,2}(N_s\mu_{sr}P_s + N_d\mu_{rd}P_d) + \sigma_n^2})K - 1$$

As a result, by regarding this strategy, the total relay power is minimized. We show this innovation in simulation section of the paper. As seen in eq. (13), the optimal transmitted power at the BS, i.e. P_s^* is linearly increased with data rate. Furthermore, at higher AN powers, the optimal signal power at the BS is linearly proportional to the AN power and increased by increasing AN power. As such, as we can see from (13), P_s^* is proportional to the inverse of λ_s. In other words, the better the first hop channel condition, the lower the power of the message signal will be sent.

Remark 3*:* It should be noted that, depending on the channel conditions, R_s may not be achievable and as a result, positive P_s and w may not be found. In this situation, the transmitter keeps silence. and we have no transmission.

A pseudocode of the overall procedure of the proposed method is presented in Fig. 2.

B. ***Relay power minimization with relay's transmitter HWI***

The actual transmitted signal at the relay node can be expressed as

$$x_R = w\left(\sqrt{P_s}\boldsymbol{h}_{sr}\boldsymbol{W}_{S,k}x_s + \sqrt{P_d}\boldsymbol{h}_{dr}\boldsymbol{W}_{d,k}x_d + n_R\right) + \eta_R^t. \quad (15)$$

The useful received signal after cancelling self-interference, i.e. x_d, at the destination is

$$y_D = \underbrace{\sqrt{P_s}w\|\boldsymbol{h}_{sr}\|\boldsymbol{h}_{rd}x_s}_{\text{Information Signal}} + \underbrace{w\boldsymbol{h}_{rd}n_r + \boldsymbol{n}_D}_{\text{AWGN Noise}} + \underbrace{\eta_{R,k}^t\boldsymbol{h}_{rd}}_{\text{Distortion Noise}}. \quad (16)$$

When, MRT transmits the weighting vectors at the BS as $\boldsymbol{W}_{S,k} = \frac{\boldsymbol{h}_{sr}^H}{\|\boldsymbol{h}_{sr}\|}$, and MRC received the weighting vectors at the UE as $\boldsymbol{W}_{d,k} = \frac{\boldsymbol{h}_{rd}^H}{\|\boldsymbol{h}_{rd}\|}$.

The achievable signal-to-interference-plus-noise ratio (SINR) at the relay and destination are expressed as

$$\gamma_R = \frac{\lambda_s P_s}{\lambda_d P_d + \sigma_n^2}, \quad (17)$$

$$\gamma_D = \frac{\lambda_w\lambda_s\lambda_d P_s}{\lambda_w {\kappa_R^t}^2\lambda_d(\lambda_s P_s + \lambda_d P_d) + \lambda_w\lambda_d\sigma_n^2 + \sigma_n^2}, \quad (18)$$

where $\lambda_w = |w|^2$, $\lambda_s = \|\boldsymbol{h}_{sr}\|^2$ and $\lambda_d = \|\boldsymbol{h}_{rd}\|^2$.

The minimization problem subject to a minimum required target rate $\hat{R}_s$ can be formulated as

$$\min_{P_s,\lambda_w} \lambda_w\left((\lambda_s P_s + \lambda_d P_d)\left(1 + {\kappa_R^t}^2\right) + \sigma_n^2\right). \quad (19)$$
$$s.t.\ R_s \geq \hat{R}_s,\ P_s > 0,\ P_d > 0,\ \lambda_w > 0$$

Here with the reason that we mentioned in section 3.1., the optimal solution of (19) is obtained when $R_s = \hat{R}_s$. By invoking (17) and (18) into (7) and after solving the equation $R_s = \hat{R}_s$ respect to λ_W, the optimal value of λ_W i.e. λ_W^* is expressed as

$$\lambda_W^* = \frac{\sigma_n^2}{\lambda_d}\left[\frac{U_3}{P_s\lambda_s - \left((\lambda_s P_s + \lambda_d P_d){\kappa_R^t}^2 + \sigma_n^2\right)U_3}\right]. \quad (20)$$
$$U_3 \triangleq \left(1 + \frac{\lambda_s P_s}{\lambda_d P_d + \sigma_n^2}\right)K - 1$$

Now, we consider the relay power minimization problem when the source power $P_s > 0$ and the destination noise power $P_d > 0$ are given. Therefore, the minimization problem subject to a minimum required target rate $\hat{R}_s$ can be formulated as

$$\min_{\substack{P_s,\\ s.t.\ P_s>0,\ P_d>0}} \lambda_W^*\left((\lambda_s P_s + \lambda_d P_d)\left(1 + {\kappa_R^t}^2\right) + \sigma_n^2\right). \quad (21)$$

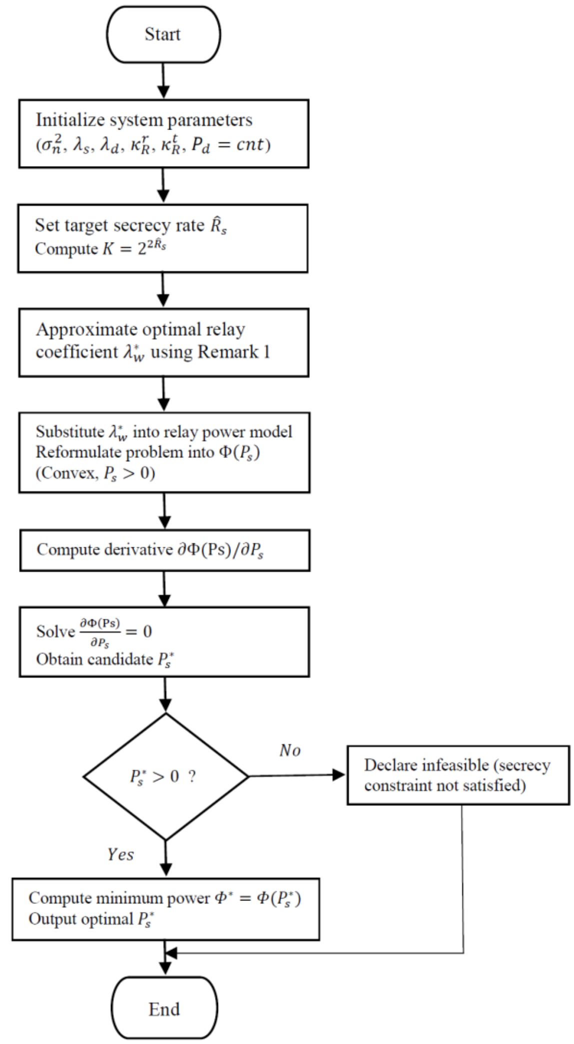

Fig. 2. Algorithm 1: A pseudocode of the overall procedure of the proposed method

For simplicity and without losing of generality, we assume that the power of P_d is constant. Then, the optimization problem is reformulated by the following unconstrained problem

$$\min_{P_s>0} \Phi(P_s)|_{P_d=cnt}, \quad (22)$$

where $\Phi(P_s) = \lambda_W^*((\lambda_s P_s + \lambda_d P_d)(1 + {\kappa_R^t}^2) + \sigma_n^2)$.

Theorem 2: $\Phi(P_s)$ is a convex function of P_s.

Proof: The proof follows from the *theorem1*

Regarding ***Remark 1*** and ***Theorem 2***, and considering that κ_R^t is a small number, the optimal point of (22) i.e., the signal power is found by solving $\frac{d\Phi(P_s)}{dP_s}|_{P_d=cnt} = 0$, and approximated by

$$P_s^* = -\frac{1}{\lambda_s K}\frac{\left((K(K-1)\sigma_n^2) + S_3\right)(\lambda_d P_d + \sigma_n^2)}{-\lambda_d P_d + (K-1)\sigma_n^2}. \quad (23)$$
$$S_3 = \sqrt{K\lambda_d P_d(K-1)\left(\lambda_d P_d\left(1 + 2{\kappa_R^t}^2\right) + \sigma_n^2\right)}$$

In LSA regime at the source and destination, by applying (12) in (23), P_s^* can be rewritten as

$$P_s^* = \frac{1}{N_s \mu_{sr} K} \times \frac{\left((K(K-1)\sigma_n^2) + S_4\right)(N_d \mu_{rd} P_d + \sigma_n^2)}{-N_d \mu_{rd} P_d + (K-1)\sigma_n^2}. \quad (24)$$

$$S_4 \triangleq \sqrt{K N_d \mu_{rd} P_d} \times \sqrt{(K-1)\left(N_d \mu_{rd} P_d\left(1 + 2{\kappa_R^t}^2\right) + \sigma_n^2\right)}$$

Using the same reasoning we used in Section 3-1 for very large antennas, (20) can be written as

$$\lambda_W^* = \frac{\sigma_n^2}{N_d \mu_{rd}} \times \left[\frac{U_4}{N_s \mu_{sr} P_s - \left((N_s \mu_{sr} P_s + N_d \mu_{rd} P_d){\kappa_R^t}^2 + \sigma_n^2\right) U_4}\right]. \quad (25)$$

$$U_4 \triangleq \left(1 + \frac{N_s \mu_{sr} P_s}{N_d \mu_{rd} P_d + \sigma_n^2}\right) K - 1$$

The optimal amplification weight is obtained after replacing (25) at (26) as

$$|W^*| = \sqrt{\lambda_W^*}. \quad (26)$$

As a result, by regarding this strategy, the total relay power is minimized. We show this innovation in simulation section of the paper. As seen in (24), the optimal transmitted power at the BS, i.e. P_s^* is linearly increased with data rate. Furthermore, at higher AN powers, the optimal transmitted power at the BS is also increased.

Remark 4: The proposed EE and power allocation schemes rely on instantaneous CSI to compute the relay amplification factor. In the absence of CSI, the instantaneous SINR and EE cannot be evaluated, rendering the closed-form optimization infeasible. However, with partial or statistical CSI, alternative stochastic or robust optimization frameworks could be employed at the cost of increased complexity and performance degradation.

IV. Numerical results and discussion

In this section, numerical examples are presented to verify the correctness of the proposed scheme. The noise variance is assumed to be -20 dB. Furthermore, we set $\mu_{sr} = \mu_{rd} = 0.2$. We mention that the secrecy rate metric represents a spectral-efficiency measure expressed in bits/s/Hz; therefore, increasing the system bandwidth naturally leads to an improvement in the achievable secrecy rate. In this work, the system performance is evaluated in terms of this spectral-efficiency-based secrecy rate metric, which enables a bandwidth-independent and scalable performance assessment.

Based on ***Theorem 1*** presented in section III, the relay transmit power is a convex function of the BS transmit power over the feasible set. This convexity behavior is clearly illustrated in Fig. 3. As we can see from Fig. 3, by increasing the imperfections in the receiver/transmitter hardware of the relay, relay average transmit power ($P_{r,T}$) increased. As such, optimum value of the transmitted signal power corresponds well to (13) when the relay has HWI on its receiving side or (24) when the relay has HWI on its transmitting side. Furthermore, as we consider from Fig. 3, within the range of optimal transmitted signal, the relay with HWI on its receiving side, has less retransmitted power than the relay with HWI on its transmitting side. This shows that the transmit hardware impairments at AF relays has more important role than their receive HWIs.

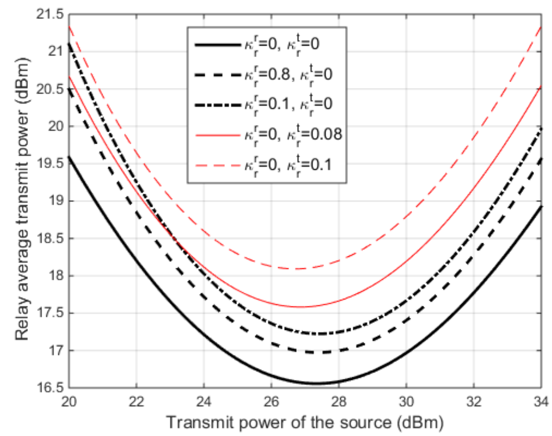

Fig. 3. Relay average power transmission ($P_{r,T}$) versus the transmit source power for different $\kappa_R^r s$ and κ_R^ts. We consider $P_d = 27.8$ dBm, $N_S = N_D = 16$ and $\hat{R}_s = 4$ bits/s/Hz

Fig. 4 depicts the $P_{r,T}$ in dBm versus target rate $\hat{R}_s$ for both cases when the relay has HWI on its receiving side and when the relay has HWI on its transmitting side and in scenario of perfect hardware ($\kappa_r^r = \kappa_r^t = 0$). Relay node is equipped with single antenna. As we can see from Fig. 4, given the higher target rate, the relay must retransmit more power. Also, at higher target rates, the relay's transmitted power increases exponentially respect to $\hat{R}_s$ specifically for higher $\kappa_r^t s$. As can be seen, the solution of the total transmit power states that most of the power is consumed by relay to satisfy a desired target rate specifically, for higher $\kappa_r^r s$ and $\kappa_r^t s$ to satisfy a desired target rate.

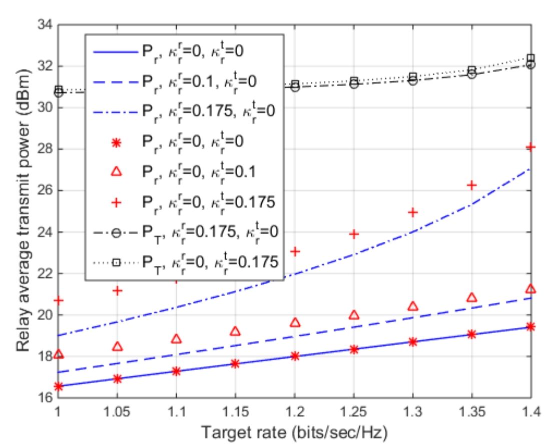

Fig. 4. Relay average power transmission ($P_{r,T}$) versus the target rate for different $\kappa_R^r s$ and κ_R^ts. We consider $P_d = 27.8$ dBm, $N_S = N_D = 16$ and $P_s = 27$ dBm

Without loss of generality, we consider a linear relaying model with a path loss exponent $n = 3$, where the source and destination are located at the first and the end of a normalised distance, respectively, and one relay node is distributed in this line (A single-relay system with independently and non-identically distributed links.). Let the distance between source and relay be $d_{sr} = d$ and between relay and destination be $d_{rd} = 1 - d$, where $d \in (0.3\, m, 0.7\, m)$. Therefore, $\mu_{sr} = d^{-n}$ and hence $\mu_{rd} = (1 - d)^{-n}$. For this scenario, we present Fig. 5 to show the effect of relay location on the average relay transmit power. It can be seen intuitively that for the relay with HWI on its receiving side at $d \simeq 0.57$ m, the average $P_{r,T}$ is minimized and for the relay with HWI on its transmitting side at $d \simeq 0.58$ m, the average $P_{r,T}$ is minimized. As such, d in scenario of perfect hardware is a little greater than that of imperfect hardware one. These results give some insights to design an EE system.

It should be noted that our analysis and simulations are conducted in a distance-normalized environment. Similar assumptions have also been adopted in related works, such as [7], [10] and [16]. The results presented in this paper can be readily justified and extended to larger-scale deployment scenarios by employing antenna arrays with higher gains and correspondingly higher power consumption.

For fixed BS and UE transmit powers, variations in the relay location significantly influence the achievable secrecy rate through their impact on the source transmit power, relay transmit power, received power at the destination, and the relative geometry of the network nodes. In Fig. 5, the relay transmit power is depicted as a function of the relay position (parameterized by distance $\boldsymbol{d}$), while $\boldsymbol{R_s}$, $\boldsymbol{P_s}$, and $\boldsymbol{P_d}$ are kept constant. As observed, the relay transmit power exhibits a decreasing–increasing trend with increasing distance, resulting in a unimodal behavior. This characteristic provides clear insight into the existence of an optimal relay location that minimizes the relay power consumption. Specifically, when the relay is placed too close to the BS, its increased separation from the destination necessitates higher transmit power, which is consistent with the results shown in Fig. 5. Conversely, when the relay is located too far from the BS, the weakened received signal from the BS forces the relay to increase its transmit power to ensure reliable delivery to the UE, again in agreement with Fig. 5.

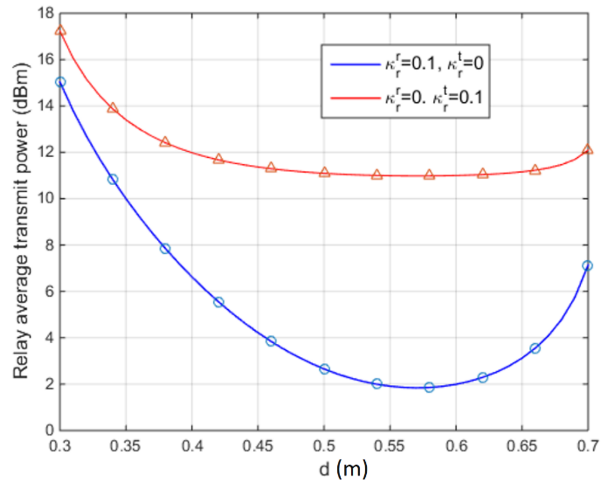

Fig. 5. Relay average power transmission ($P_{r,T}$) versus the distance between relay and source (d). We set $P_s = 27.8$ dBm and $\hat{R}_s = 1.2$ bits/s/Hz.

Table I summarizes the considered HWI models and their impact on the system performance. Specifically, receiver HWIs at the relay introduce additive distortion noise proportional to the received signal power, which increases the relay's average transmit power and leads to a higher optimal source transmit power as the impairment level grows. In contrast, transmitter HWIs cause distortion proportional to the relay transmit power, resulting in a faster growth of the relay power consumption compared to the receiver-side HWIs. The perfect hardware case is included as a benchmark, providing a lower bound on the required transmit power.

Table 1: HWIs and their impact on system performance

Impairment Type	Parameter	Location	Effect on System Model	Key Result/Observation
Receiver HWI	κ_R^r	Relay receiver	Adds distortion noise proportional to received signal power	Increases relay average transmit power $P_{r,T}$; higher $\kappa_R^r \rightarrow$ higher optimal P_s^*
Transmitter HWI	κ_R^t	Relay transmitter	Introduces distortion proportional to relay transmit power	Causes faster growth of $P_{r,T}$ compared to receiver impairment
Perfect hardware (benchmark)	$\kappa_R^r = \kappa_R^t = 0$	Relay	No distortion noise	Lowest required transmit power; serves as lower bound
Noise variance	σ_n^2	All receivers	Thermal noise floor	Fixed and known; does not affect convexity
Target secrecy rate	$\hat{R}_s$	System constraint	Defines secrecy threshold $K = 2^{2\hat{R}_s}$	Higher $\hat{R}_s$ significantly increases optimal power

Moreover, the noise variance is assumed fixed and known, and thus does not affect the convexity of the optimization problem, while a higher target secrecy rate significantly increases the required optimal transmit power.

V. Conclusions

In the existing literature, only a few studies have examined the effects of HWIs on energy efficiency and calculating of optimal transmit power in security based transmission. Moreover, there is limited information available regarding this impact on untrusted relay networks. In this paper, by taking HWIs into consideration, we proposed an optimal signal power strategy to minimize the energy efficiency of a cooperative wireless network which includes a source, a destination and an untrusted AF relay. Based on our EE solutions, new closed-form expressions were derived for the optimal signal power with Rayleigh fading channels. The expressions effectively characterize the impact of HWIs. The results effectively characterize the impact of HWIs on higher target rate, that the relay must retransmit more power. As a result, HWIs should be taken into account when developing high rate systems such as LTE-Advanced, 5G and B5G networks. Furthermore, we have demonstrated that the optimal transmit power is inversely proportional to the first-hop channel gain; hence, the better the quality of this channel, the more significant its impact in enabling signal transmission with lower power.

References

[1] M. Swain, M. Panda and P. K. Sahoo, "Performance Analysis of Relays used in Next-Generation Wireless Communication Networks using the Hata Model," *2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, Bhubaneswar, India, pp. 1-4, 2024, doi: 10.1109/ODICON62106.2024.10797619.

[2] C. Dutriez, O. S. Oubbati, C. Gueguen and A. Rachedi, "Energy Efficiency Relaying Election Mechanism for 5G Internet of Things: A Deep Reinforcement Learning Technique," *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, Dubai, United Arab Emirates, pp. 1-6, 2024, doi: 10.1109/WCNC57260.2024.10570813.

[3] F. Irram, M. Ali, M. Naeem, and S. Mumtaz, "Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions," *J. Netw. Comput. Appl*., vol. 206, p. 103431, Oct. 2022, doi: 10.1016/j.jnca.2022.103431.

[4] H. Saedi,, A. Mohammadi, and A. Kuhestani, "Secure communication with a multiple-antennas untrusted relay in presence of randomly distributed adversary jammers," *Physical Commun.*, vol. 66, Sept. 2024, doi: https://doi.org/10.1016/j.phycom.2024.102463.

[5] M. Ragheb, S. M. Safavi. Hemami, A. Kuhestani, D. W. K. Ng and L. Hanzo, "On the Physical Layer Security of Untrusted Millimeter Wave Relaying Networks: A Stochastic Geometry Approach," *IEEE Trans. Inf. Forensics and Security*, vol. 17, pp. 53-68, 2022, doi: 10.1109/TIFS.2021.3131028.

[6] A. Kuhestani, A. Mohammadi, K.-K. Wong, P. L. Yeoh, and M. Moradikia, "Optimal power allocation by imperfect hardware analysis in untrusted relaying networks," *IEEE Trans. Wireless Commun*., vol. 17, no. 7, pp. 4302–4314, Jul. 2018, doi: 10.1109/TWC.2018.2822286.

[7] H. Zarrabi, A. Kuhestani and M. Moradikia, "EE-RS and PA for untrusted relay network at high signal-to-noise ratio regime," *IET Commun.*, vol. 10, no. 16, pp. 2143-2148, Nov. 2016, doi: https://doi.org/10.1049/iet-com.2016.0367.

[8] C. Dianxia, M. Xiaoshan, Y. Lin, Y. Kan and F. Zhiyong, "Cooperative relaying and jamming design for secure LPWAN wireless communication," *China Commun.*, vol. 22, no. 4, pp. 100-116, Apr. 2025, doi: 10.23919/JCC.fa.2024-0156.202504.

[9] H. Shi and G. Wang, "Physical Layer Security in the Untrusted EH Relay Networks with the Cooperative Jammer," *2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 2020, pp. 899-903, doi: 10.1109/WCSP49889.2020.9299686.

[10] H. Yu and I.-G. Lee, "Physical layer security based on NOMA and artificial jamming for MISOSE channels with an untrusted relay," *Future Generation Computer Systems*, vol. 102, Pages 611-618. Jan. 2020, doi: https://doi.org/10.1016/j.future.2019.09.019.

[11] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2701–2718, Sept. 2021., doi: 10.1109/JSAC.2021.3064662.

[12] J. Li, X. Yin, X. Ding, Z. Yang, N. Ye and K. Yang, "Nonideal energy efficiency optimization based on MIMO communications," *IEEE Internet Things J.*, vol. 12, no. 13, pp. 23975-23987, 1 Jul. 2025, doi: 10.1109/JIOT.2025.3554678.

[13] P. Zhao, W. Zhao, H. Bao and B. Li, "Security energy efficiency maximization for untrusted relay assisted NOMA-MEC network with WPT," *IEEE Access*, vol. 8, pp. 147387-147398, 2020, doi: 10.1109/ACCESS.2020.3015786.

[14] R. Yao, F. Xu, T. Mekkawy, and J. Xu, "Optimised power allocation to maximise secure rate in energy harvesting relay network," *Electronics Letters*, vol. 52, no. 22, Pages 1879-1881, Oct. 2016, doi: https://doi.org/10.1049/el.2016.3201.

[15] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi and L. Hanzo, "RIS-Aided Secure Millimeter-Wave Communication Under RF-Chain Impairments," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 952-963, Jan. 2024. doi: 10.1109/TVT.2023.3307451.

[16] M. Letafati, A. Kuhestani, and H. Behroozi, "Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things," *IEEE Trans. Inf. Forens. and Security*, vol. 15, pp. 2856–2868, Mar. 2020. doi: 10.1109/TIFS.2020.2978627.

[17] V. Shahiri, A. Kuhestani, and L. Hanzo, "Short-packet amplify-andforward relaying for the internet-of-things in the face of imperfect channel estimation and hardware impairments," *IEEE Trans. Green. Commun. and Net*., 2022, doi: 10.1109/TGCN.2021.3092067.

[18] K.-H. Lee, K. Lim, and B. C. Jung, "STEALTH: Space-time encryption via constellation hiding for MIMO two-way untrusted relay systems," *IEEE Internet Things J*., vol. 12, no. 15, pp. 30319 - 30334, Aug. 2025, doi: 10.1109/JIOT.2025.3571736.

[19] S. Zhao, X. Zhu, Y. Zhang, Z. Zhang and Y. Shen, "Joint RIS and beamforming design for secure and energy-efficient two-way relay communications," *IEEE Trans Mobile Comput.*, vol. 24, no. 8, pp. 7440-7457, Aug. 2025, doi: 10.1109/TMC.2025.3549445.

[20] Rahmani and N. Yazdani, "5G-R framework for high-speed rail connectivity using AI and edge computing," *Int. J.*

Ind. Electron. Control Optim., Articles in Press, 2025, doi: 10.22111/ieco.2025.52762.1709.
[21] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri and F. Khan, “Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks,” *IEEE Access*, vol. 9, pp. 42583-42592, 2021, doi: 10.1109/ACCESS.2021.3065760.
[22] M. Kazemi, A. Mohammadi and T. M. Duman, “Analysis of DF relay selection in massive MIMO systems with hardware impairments,” *IEEE Trans. Veh. Technol*, vol. 69, no. 6, pp. 6141-6152, June 2020, doi: 10.1109/TVT.2020.2968874.
[23] T. Schenk, RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation. New York, NY, USA: Springer, 2008.
[24] H. Holma and A. Toskala, *LTE for UMTS: Evolution to LTE Advanced*, 2nd ed. Hoboken, NJ, USA: Wiley, Mar. 2011.
[25] A.-A. A. Boulogeorgos, E. N. Papasotiriou, and A. Alexiou, “Analytical performance assessment of THz wireless systems,” *IEEE Access*, vol. 7, pp. 11436–11453, 2019, doi: 10.1109/ACCESS.2019.2892198.
[26] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014, doi: 10.1109/SURV.2014.012314.00178.
[27] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008, doi: 10.1109/TIT.2008.921908.
[28] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 1984.

Appendix A

MOHAMMAD RAGHEB received the Ph.D. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2022. He is an Invited Professor of Telecommunication Engineering at Qom University of Technology, Qom, Iran. His research interests include physical-layer security of wireless communications, millimeter-wave communication, and massive MIMO systems.

ALI KUHESTANI (Member, IEEE) received the Ph.D. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2017. He is an Associate Professor in the Communications and Electronics Department, Faculty of Electrical and Computer Engineering, Qom University of Technology, Iran. His research interests include physical-layer security of wireless communications, the Internet of Things, millimeter-wave communication, massive MIMO systems, and space-time coding.

MOHAMMADREZA KESHAVARZI received his Ph.D. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran,in 2009. Since 2012, he has been with the Iran Telecommunication Research Center (ITRC) in Tehran, Iran as an assistant professor. His research interests include physical-layer security of wireless communications, Internet of Things, and MIMO systems.