Cooperative Secure Transmission Relying On the Optimal Power Allocation in the Presence of Untrusted Relays, a Passive Eavesdropper and Hardware Impairments

Majid Moradikia, Hamed Bastami, Ali Kuhestani, *Student Member, IEEE,*
Hamid Behroozi, *Member, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—In this work, by considering a variety of realistic hardware impairments, we aim to enhance the security of a cooperative relaying network, where a source intends to transmit its confidential information to a destination in the presence of a group of untrusted amplify-and-forward relays, as potential eavesdroppers (Eves), and an entirely passive multiple-antenna aided Eve. Our goal is to safeguard the information against these two types of eavesdropping attacks, while simultaneously relying on the untrusted relays to boost both the security and reliability of the network. To reach this goal, we propose a novel joint cooperative beamforming, jamming and power allocation policy to safeguard the confidential information while concurrently achieving the required quality-of-service at the destination. We also take into account both the total power budget constraint and a practical individual power constraint for each node. Our optimization problem can be split into two consecutive sub-problems. In the first sub-problem, we are faced with a non-convex problem which can be transformed into the powerful difference of convex (DC) program. A low-complexity iterative algorithm is proposed to solve the DC program, which relies on the constrained concave-convex procedure (CCCP). We further introduce a novel initialization method, which is based on a feasible point of the original problem obtained from a novel iterative feasibility search procedure, rather than an arbitrary (infeasible) point as in the conventional CCCP. The second sub-problem of our optimization problem is a convex optimization problem and can be solved efficiently adopting the classic interior point method. The numerical results provided illustrate that although the trusted relaying scenario outperforms the untrusted relaying for small and medium total power budgets, however, by increasing the total power budget, the secrecy performances of both the trusted and untrusted relaying converge to the same. Additionally, by equally sharing the total impairments at the relays between the transmitter and the receiver the best secrecy performance is presented.**

***Index Terms*—Physical layer security, Untrusted relay, Passive eavesdropper, Hardware impairments, Cooperative beamforming and jamming, Optimal power allocation.**

I. Introduction

IN recent decades, physical layer security (PLS) has received a lot of attention due to its capability to establish secure transmission without relying on conventional upper-layer cryptography methods. From an information theoretic point of view, when the channel gain of the legitimate link is stronger than that of the wiretap link, the legitimate receiver can correctly decode the secret information while the eavesdroppers (Eves) cannot [1]. To reveal the benefits of PLS, Mukherjee *et al.* in [2] as well as Zou *et al.* in [3] have comprehensively reviewed a suite of efficient PLS solutions. On the other hand, in order to have a perfect security over the internet-of-things (IoT) networks, the work of [4] have reviewed several PLS protocols and discussed about the challenges ahead for applying these PLS techniques. Among the proposed PLS solutions, relay-aided transmission which is applicable for wireless sensor networks and the IoT has recently attracted much interest [5]-[19]. The authors of [5]-[9] have assumed that only one node is selected as relay. Whereas, in order to take full advantage of the multiple intermediate helpers, two well-known techniques cooperative beamforming (CB) and cooperative jamming (CJ) widely suggested in the literature [10]-[21]. The idea behind the CB policy is to boost the channel quality of the legitimate link by focusing a directional beam on the legitimate receiver. A somewhat impractical assumption considered in the literature is that the channel state information (CSI) of the Eve is perfectly known at the transmitter [10]-[15], [17]. However, a few articles have also studied the more realistic scenario of an *entirely passive Eve*, where the CSI and location of the Eve cannot be obtained by the secure communication network [16]. To circumvent this issue, the CJ technique can be invoked for isotropically propagating artificial noise (AN) to degrade the quality of the wiretap link [10], [16], [17]. The CJ regime relies on the following three different techniques: (1) source-assisted cooperative jamming (SACJ), where a combination of information bearing signal and AN is radiated by the source [19], [20], (2) friendly-user assisted cooperative jamming (FACJ) in which one of the legitimate nodes of the network is enlisted to serve as a jammer [11]-[17], (3) destination-assisted cooperative jamming (DACJ), where the AN is injected by the destination [21], [22]. Notably, a more robust secure transmission is achievable when the network under study enjoys from both the CJ and CB techniques [10]-

M. Moradikia is with the Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran, e-mail: m.moradikia@sutech.ac.ir.

H. Bastami, *et al.* are with the Electrical Engineering Department, Sharif University of Technology, Tehran, Iran, e-mails: hamed.bastami@ee.sharif.edu, kuhestani@sharif.edu, behroozi@sharif.edu.

Lajos Hanzo is with the University of Southampton, Southampton SO17 1BJ, U.K, e-mail: hanzo@soton.ac.uk.

[13], [16], [17].

From the security point of view, an *untrusted relay* can be exploited for improving the reliability of transmission, while concurrently it may intercept the confidential information for fulfilling passive attacks [17], [22]-[25]. Some practical networks including untrusted relays are ultra-dense heterogeneous wireless networks as well as ad-hoc networks and IoT networks. In recent years, several articles have investigated the secrecy performance of communication networks in the face of a single [22] or multiple amplify-and-forward (AF) untrusted relays [17], [10]-[25]. Furthermore, the authors of [10], [25] studied the achievable secrecy performance when relying on opportunistic relaying. By contrast, the authors of [17], [24] invoked the distributed CB for boosting the secrecy performance. However, only [17] and [25] considered the external Eves, having known location, besides of the untrustworthy relay nodes. To overcome these combined attacks, a joint CB and CJ technique has been proposed by Moradikia *et al.* [17], where the jammer and source powers are optimized in the presence of a single antenna Eve whilst assuming a known CSI. Moradikia *et al.* [17] also considered a sum power constraint at the relays, which is not a realistic assumption. It is more realistic to optimize the power of each relay. To reach this goal, by assuming that the Eve's CSI is unknown, a cooperative AN propagation strategy, subjected to the individual power constraint of each node was proposed in [16]. However, this system model is only applicable to trusted relaying and has been designed without judicious source and jamming power allocation. More explicitly, all the aforementioned articles optimistically assumed ideal hardware for the entire communication system, which is an unrealistic assumption.

In real world, the hardware is always imperfect, suffering from intrinsic impairments like I/Q imbalance, oscillator phase noise, high power amplifier nonlinearities, imperfect filters, etc. [26]-[28]. From engineering perspective, the extent of these impairments depends on the quality of the hardware utilized in the radio-frequency (RF) sections. These inevitable impairments may become particularly grave in cooperative relaying networks relying on low-cost intermediate nodes of sensor or ad-hoc networks. Note that although the hardware impairments (HIs) can be reduced by analog and digital signal processing techniques [26], they cannot be completely eliminated. Accordingly, Björnson *et al.* [27] revealed that the residual HIs can be adequately modeled by additive noises both at the transmitter and receiver [27], [28]. While most of the articles in the area of security have considered the assumption of perfect hardware, the influence of some type of imperfections such as I/Q imbalance in the presence of an external Eve has been investigated by Boulogeorgos [29]. Furthermore, since all nodes may have HIs, the authors of [30] optimized the achievable secrecy rate of an untrusted relaying system. More explicitly, optimal power allocation (OPA) and some hardware design aspects have been taken into account in [30], but only a single untrusted relay was relied upon and no passive Eve was considered. The results of [30] highlight that by appropriately sharing the tolerable HIs across the transmission and reception RF front ends of each node, the system's secrecy performance is enhanced. In a nutshell, most investigations in the area of secure communication have assumed perfect transceiver hardware [5]–[25], or only considered the effect of I/Q imbalance [29] in the presence of a single external Eve, or only considered a single untrusted relay without any passive Eve [23]. Hence this article goes beyond these investigations by taking into account the HIs in a more general network with the aim of improving the PLS design.

To elaborate a little further, by considering a variety of realistic HIs, we consider a cooperative network including a source, a destination, several untrusted relays and an entirely passive Eve, whose location is unknown. The potent passive Eve has multiple antennas, but we assume all the remaining nodes, are equipped with a single antenna. Considering this communication network, the contributions of our work are summarized as follows:

- With the aim of improving the system's PLS, we propose a joint CB and CJ scheme, where each node's power is optimized. To protect the security of transmission during the first phase, we propose to choose an appropriate jammer among the untrusted relays and the destination. In the second phase of transmission, the idle source is configured to operate as a jammer and concurrently, part of the untrusted relays' power is assigned to inject AN in the network, which is designed to be in the null space of the relay-destination channel.
- For this network design, we consider both the total power constraint for the whole network and individual power constraint at each node. Accordingly, with the objective of achieving a minimum required quality-of-service (QoS) at the destination, we minimize the power allocated to both of the cooperative phases and simultaneously, we maximize the total power assigned to the different jamming sources to improve the network security.
- The corresponding optimization problem can be split into two consecutive sub-problems. In the first sub-problem, we are faced with a non-convex problem which can be transformed into the difference of convex (DC) program [31], [32]. We propose a low-complexity iterative algorithm for solving the DC program, which is based on the constrained concave-convex procedure (CCCP) [33], [34]. The second sub-problem is a convex optimization problem and can be solved using interior point optimization.
- For the first sub-problem, we further present a new initialization procedure that is based on a feasible point of the original problem obtained from a novel iterative feasibility search procedure, rather than an arbitrary (infeasible) point as in the conventional CCCP [33], [34]. Consequently, we can guarantee for the algorithm to avoid any failure due to infeasibility, but also all the outcomes obtained from aforesaid CCCP, belong to the original feasible set of the DC program.
- Our numerical results highlight that the trusted relaying scenario outperforms the untrusted relaying for small and medium total power budgets. However, as the total

power budget is increased, the secrecy performance of the trusted and untrusted relaying becomes identical. Furthermore, by equally sharing the total affordable impairments at the relays between the transmitter and the receiver results in the best secrecy performance.

Eventually, in order to turn this work into a well-rounded treatise, we have provided a comprehensive historical perspective, illustrated in Fig. 2 at the next page. This figure reveals the entire evolution of PLS research and particularly focused on those papers that are close in spirit to ours.

II. System model

An AF cooperative network is illustrated in Fig.1 wherein a source S wants to deliver its confidential information to the destination D in the presence of a passive Eve E and N intermediate untrusted relays in the set $\boldsymbol{R} \triangleq \{R_1, R_2, ..., R_N\}$. In fact, the untrusted relays in our network are semi-trusted, i.e. they are trusted to convey the accurate CSIs to S via relay-aided cooperation, while they are untrustworthy in terms of retransmitting the confidential information. In other words, although $\boldsymbol{R}$ would transmit the info towards S, it infer the info for itself, as well. It should be emphasized that the term "$curious\ node$" in this paper refers to both the untrusted relays and the passive Eve. We further assume that the untrusted relays are close to each other[11]-[13] and can decipher the information signal based on their own observation by adopting selection combining (SC) [25], whilst the passive Eve tries to elicit more information through combining its own observations in two consecutive phases. All the nodes except for the Eve, which is equipped with N_E antennas, possess a single antenna and operate in a half-duplex mode. It is also assumed that there is no straight path between S as well as D and there is no message passing between any of the relays. Furthermore, we assume having quasi-stationary flat-fading channels, which are shown in Fig.1 and time-division duplex (TDD) mode is adopted so that the channels' reciprocity is satisfied. The jammer node J intends to confuse the curious nodes via emitting jamming. As such, during the first phase, S transmits the intended signal at power $0 < P_s \leq P_T$ and in the meantime, the jammer selected in phase I (J_1) transmits Gaussian noise at a power of $0 < P_{J_1} \leq \bar{P}_{J_1}$ to confuse both the Eve E and the untrusted relays . If, for ease of exposition we assume that $J_1 = R_N$ is selected from $\boldsymbol{R}$, the $N-1$ other relay nodes of the set $\boldsymbol{R}_{-1} \triangleq \{R_1, R_2, , R_{N-1}\}$ can take part in cooperative relaying during phase II. During the second phase of data transmission, the untrusted relays within $\boldsymbol{R}_{-1}$ forward the received signal to D with at a power of $\boldsymbol{P}_{R-1} \triangleq [P_{R_1}, P_{R_2}, , P_{R_{N-1}}]^T \in \mathbb{R}^{(N-1)\times 1}$ using distributed beamforming where P_{R_l} describes the transmit power at R_l, $\forall l \in L$ with $L \triangleq 1, 2, , N-1$. Notably, in the second phase, since the untrusted relays operate in half-duplex mode, they cannot overhear the data signal. But another opportunity is provided for E to glean confidential information. Hence, in this phase we only have to combat the attack of the passive Eve. In this regard, the jammer selected in the second phase (J_2) transmits jamming at a power of $0 < P_{J_2} \leq \bar{P}_{J_2}$ for contaminating Eve's link.

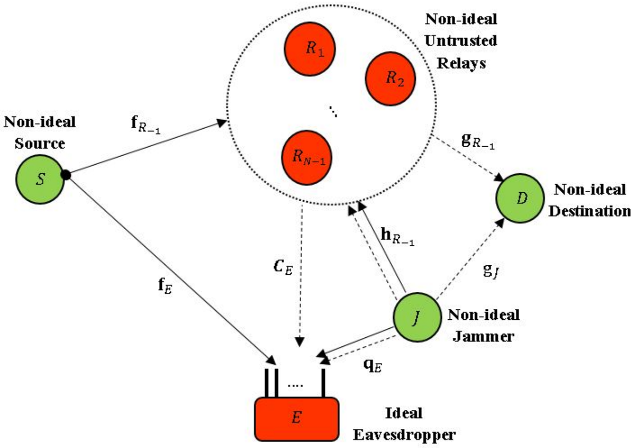


Fig. 1. Secure relaying in the presence of multiple untrusted relays and a passive Eve. During the first phase, an appropriate jammer J is chosen among the untrusted relays and destination, while in the second phase of data retransmission, the idle source is forced to work as a jammer. The solid and dashed lines depict the first and second phases of transmission, respectively.

Concerning the jammer selection design, as it will be discussed in Section III. A, in phase II, we activate node S to serve asJ_2, rather than remaining silent in this phase. We also involve the hybrid jamming scheme of [17] in phase I, which switches between the DACJ and FACJ strategies. To elaborate, in the DACJ strategy, D plays the role of jammer and all the N untrusted relays listen to the signal. Remarkably, due to the half-duplex mode, DACJ can only be exploited in phase I. In phase II, D listens for its signal, hence it cannot participate in the jammer selection procedure anymore. By contrast, in the FACJ strategy, one of the intermediate relay nodes is selected and plays the role of a jammer while the other $N-1$ untrusted relay nodes listen to the signal. We also note that using FACJ solely sacrifices a single relay node and modestly decreases the corresponding array gain. Furthermore, this policy requires the relay's CSIs, imposing a large overhead on the system and consequently may not be applicable to a large number of relays. However, because of the existence of several curious nodes constituted by the untrusted relay nodes and the passive Eve, whose CSIs are time-varying the FACJ policy may be more capable of further increasing the secrecy rate than the DACJ.

A. Transceiver impairments

The residual HIs may also be modelled as extra noise [26], [27], which imposes a mismatch between the desired signal we aim to transmit and the actually emitted signal. Now, in this section, inspired by the generalized system model of [27], the residual transceiver impairments at node i, $i \in \{S, R_l \,\forall l \in L, D\}$ are taken into account. Notably, we focus on the specific Eve resulting in the worst-case secrecy performance, namely when the signal received at E is only contaminated by extra thermal noise. The experimental results of [28] have investigated that these distortion noises are well-approximated as Gaussian distribution owing to the central limit theorem. The variance of the resultant noise at the ith

1949 Shannon [39] investigated the PLS problem from an information-theoretic perspective for the first time.

1975 Wyner in [40] introduced the degraded wiretap model and the concept of secrecy capacity which is defined as the maximum transmission rate from the source to the legitimate destination for keeping the information leakage at the eavesdroppers negligible.

1978 Csiszár and Cheong respectively in [41] and [42] generalized the idea of [40] to non-degraded wiretap channel and degraded Gaussian version of wiretap channel.

2001 Oohama in [43] showed for the first time that if the system utilizes an untrusted relay, a positive secrecy rate can be achieved.

2008 He *et al.* in [44] found that if the DACJ or FACJ is deployed in an untrusted relaying system, a positive secrecy rate is indeed achievable.

2009 He *et al.* in [45] studied the achievable secrecy rate for the untrusted relay channel from an information theoretic view and also proceed to investigate the question that if cooperative transmission with an untrusted relay node can ever be beneficial?

2010 Dong *et al.* [46] addressed the PLS problem of a trusted relaying network relays in the presence of one or more eavesdroppers, having perfectly known CSI. The strategy adopted in the paper is to obtain the optimal values of the source power and relay weights for maximizing the secrecy rate subject to a total transmit power constraint.

2011

Li *et al.* in [47] proposed an extension for [46] where an optimal solution was acquired rather than suboptimal solution of [46].

Huang *et al.* in [48] proposed a cooperative jamming strategy for a trusted MIMO relaying system in the presence of an external multi-antenna aided Eve. Cases involving both known and unknown Eve's CSI were investigated. In the case of known Eve's CSI, the authors studied the joint design of the jamming beamformer and the power allocation to maximize the achievable secrecy rate subjected to both total and individual power constraints. While if the Eve's CSI is unknown, first a part of source power should be allocated for guaranteeing a fixed target rate required at the legitimate destination, and then the remaining part can be assigned to jam the eavesdropper.

Jeong *et al.* in [49] studied a joint cooperative beamforming, accomplished by both the multi-antenna source and multi-antenna relay, to secure against the passive eavesdropping attack by the single untrusted relay node. In this work no external Eve was considered. The strategy adopted in the paper is to maximize the secrecy rate under both total and individual power constraints while no judicious power allocation is applied for the source.

2013

Zou *et al.* in [7] proposed an opportunistic relay selection to improve the tradeoffs between the security and reliability, in a trusted cooperative wireless network. In the scenario considered in this paper only a single antenna Eve has been considered. Furthermore, the authors assume that no jammer is deployed and the entire source's power budget is used for its transmission.

Yang *et al.* in [14] studied the cooperative secure beamforming for a trusted relaying network in the presence of multiple non-colluding single-antenna eavesdroppers whose CSI are perfectly known. The strategy adopted in the paper is to maximize the secrecy rate under both total and individual relay power constraints while no judicious power allocation is applied for the source.

Wang *et al.* in [12], suggested a joint cooperative beamforming and jamming strategy to enhance the PLS of a trusted single-antenna-assisted two-way relaying network in the presence of a single-antenna Eve. Thus, under the conditions of both with and without Eve's CSI, two various schemes were proposed, resulting in increasing the secrecy sum rate (SSR) of the two terminals. Both schemes aim to achieve the optimal beamforming weights adopted by each relay node, subjected to individual power constraint of each cooperative node. Additionally, no judicious power allocation was considered in this paper.

Björnson *et al.* [26] revealed that the achievable rate of a cooperative communication is limited due to the intrinsic impairments of the hardware equipment used in the network.

Assuming that the Eve's CSI is unknown, a cooperative AN strategy, subjected to the individual power constraint of each node was proposed in [16]. However, this system model is only applicable to trusted relaying and has been designed without judicious source and jamming power allocation. The authors have optimistically assumed ideal hardware for the entire communication system.

2014 Mo *et al.* in [50] generalized the work of [49] for a two-way relaying system in which two source nodes intend to exchange the information with the aid of a multi-antenna untrusted relay node. The goal is to maximize the secrecy sum rate via jointly optimizing the source and relay beamformers.

2014

Wang *et al.* in [51] proposed a robust joint cooperative beamforming (CB) and cooperative jamming (CJ) to address the PLS of an amplify-and-forward (AF) trusted relaying network despite the imperfect channel state information (CSI) of the multiple multi-antenna eavesdroppers.

2015

Wang *et al.* in [13] have considered a trusted relaying network in the presence of an external single-antenna aided Eve, having known CSI. Although, in their design, they considered a judicious source power allocation to achieve a better secrecy rate, the considered sum power constraint at the relays which is far from a realistic assumption. This paper also has considered the unrealistic assumption of ideal hardware for the communication system.

Wang *et al.* in [6] proposed joint relay and jammer selection approach to enhance the PLS of a trusted cooperative network to tackle with the passive attack performed by an external Eve whose CSI is aggravated by feedback delay. In this paper only a single antenna Eve has been considered. Furthermore, no power allocation strategy is considered in this paper and it is assumed that both jammer and source utilize the whole of their power budget for their transmission.

Wang *et al.* in [11] investigated the PLS problem of a trusted decode-and-forward (DF) relaying network in which a potential Eve, whose channel distribution information (CDI) is known, intends to intercept the confidential message. To combat with the eavesdropping attack, an opportunistic relaying along with artificial jamming scheme was proposed where the best cooperative node is selected to forward the information signal while the others emit AN to confound the Eves. The authors further investigated the optimal power allocation between the confidential signal and jamming signals with the aim of maximizing the ergodic secrecy rate (ESR).

Xiong *et al.* in [52] investigated the PLS problem of a scenario where a pair of legitimate user aims to communicate with the aid of an untrusted relay node. In this scenario, the source, relay, and destination are each equipped with multiple antennas. In this paper, with the aim of maximizing the secrecy rate, the authors proposed a joint destination aided cooperative jamming and precoding design where the source, relay, and destination precoding matrices, under a total power constraint, are jointly optimized.

2016

Yang *et al.* in [18] investigated the PLS problem of a scenario where a pair of legitimate user intends to communicate with the aid of a trusted MIMO relay in the presence of multiple single antenna Eves. The authors assumed that the only imperfect knowledge of the Eves' CSI is available. Given that, the secrecy strategy adopted in the paper is to jointly optimize the source power, the AF relaying weights and the covariance of the AN induced by the relay, for maximizing the SINR received at the intended receiver, subjected to a set of robust secrecy constraints.

Zhu *et al.* in [53] investigated the impact of a particular type of imperfection, i.e., phase noise, on the secrecy performance of downlink massive MIMO systems in the presence of a passive multiple-antenna eavesdropper.

Ali *et al.* in [54] studied the impact of jammer and relay locations on the achievable secrecy rate of a cooperative relaying network deploying an untrustworthy relay. The system considered in this paper deploys a friendly jamming strategy where the jamming signal is known a priori at the intended receiver.

Atallah *et al.* in [24] investigated the secrecy performance of an AF relaying network where the general case of both trusted, untrusted relay nodes together with a wire-tapper was considered. The untrusted relays collaborate with the wire-tapper extract the information. The authors studied both distributed beamforming (DBF) and opportunistic relaying (OR) techniques to combat with these attacks.

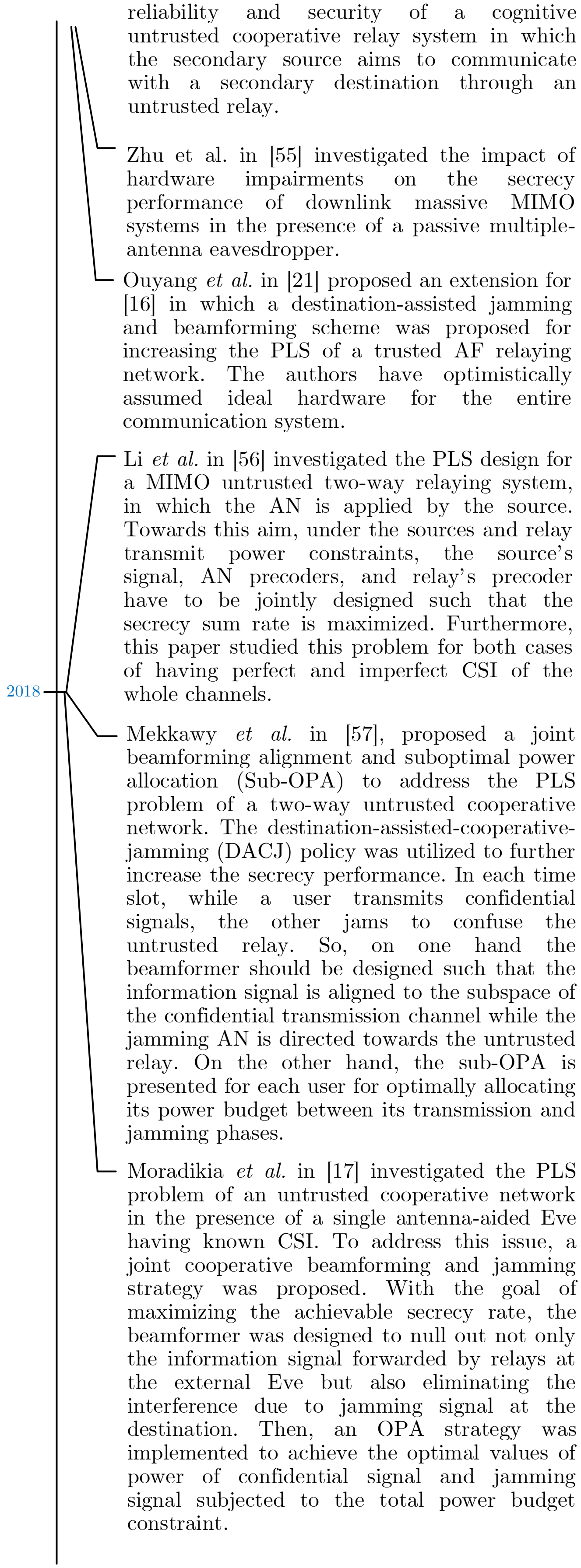
Kuhestani *et al.* in [25] have studied the energy-efficient (EE) relay selection (RS) and power allocation (PA) to minimize the power consumed by the network subjected to a minimum required secrecy rate. The authors assumed the system was relied upon a single untrusted relay without considering any passive Eve.

Boulogeorgos *et al.* in [29] have investigated the impact of some type of imperfections such as I/Q imbalance on the PLS design of a system where an external Eve would jeopardize the security of the network.

2017

Guo *et al.* in [10] proposed a joint cooperative beamforming and jamming mechanism to enhance the physical layer security of trusted DF cooperative relaying network against the passive attack by an external Eve under two assumptions of the wiretap link's CSI. With the aim of achieving the maximum achievable secrecy rate, the authors further studied the OPA among source, relays, and jammer nodes.

Chen *et al.* in [22], studied the tradeoff



reliability and security of a cognitive untrusted cooperative relay system in which the secondary source aims to communicate with a secondary destination through an untrusted relay.

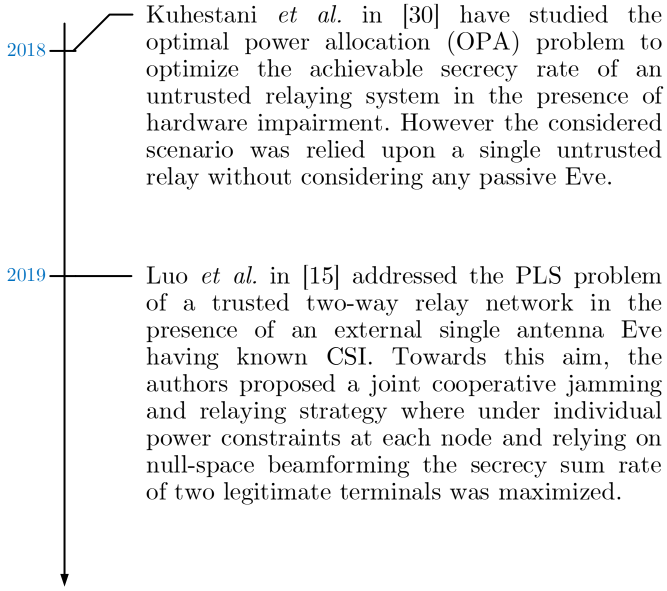
Zhu et al. in [55] investigated the impact of hardware impairments on the secrecy performance of downlink massive MIMO systems in the presence of a passive multiple-antenna eavesdropper.

Ouyang *et al.* in [21] proposed an extension for [16] in which a destination-assisted jamming and beamforming scheme was proposed for increasing the PLS of a trusted AF relaying network. The authors have optimistically assumed ideal hardware for the entire communication system.

Li *et al.* in [56] investigated the PLS design for a MIMO untrusted two-way relaying system, in which the AN is applied by the source. Towards this aim, under the sources and relay transmit power constraints, the source's signal, AN precoders, and relay's precoder have to be jointly designed such that the secrecy sum rate is maximized. Furthermore, this paper studied this problem for both cases of having perfect and imperfect CSI of the whole channels.

Mekkawy *et al.* in [57], proposed a joint beamforming alignment and suboptimal power allocation (Sub-OPA) to address the PLS problem of a two-way untrusted cooperative network. The destination-assisted-cooperative-jamming (DACJ) policy was utilized to further increase the secrecy performance. In each time slot, while a user transmits confidential signals, the other jams to confuse the untrusted relay. So, on one hand the beamformer should be designed such that the information signal is aligned to the subspace of the confidential transmission channel while the jamming AN is directed towards the untrusted relay. On the other hand, the sub-OPA is presented for each user for optimally allocating its power budget between its transmission and jamming phases.

Moradikia *et al.* in [17] investigated the PLS problem of an untrusted cooperative network in the presence of a single antenna-aided Eve having known CSI. To address this issue, a joint cooperative beamforming and jamming strategy was proposed. With the goal of maximizing the achievable secrecy rate, the beamformer was designed to null out not only the information signal forwarded by relays at the external Eve but also eliminating the interference due to jamming signal at the destination. Then, an OPA strategy was implemented to achieve the optimal values of power of confidential signal and jamming signal subjected to the total power budget constraint.



Kuhestani *et al.* in [30] have studied the optimal power allocation (OPA) problem to optimize the achievable secrecy rate of an untrusted relaying system in the presence of hardware impairment. However the considered scenario was relied upon a single untrusted relay without considering any passive Eve.

Luo *et al.* in [15] addressed the PLS problem of a trusted two-way relay network in the presence of an external single antenna Eve having known CSI. Towards this aim, the authors proposed a joint cooperative jamming and relaying strategy where under individual power constraints at each node and relying on null-space beamforming the secrecy sum rate of two legitimate terminals was maximized.

Fig. 2. Timeline of PLS researches

node is commensurate with the signal power at the corresponding antenna [28]. In the following, for ease of exposition, we have assumed that the FACJ strategy is selected in the first phase and discuss the DACJ case, wherever it is needed. Accordingly, if we denote the impairments at transmission and reception, respectively by η_i^t and η_i^r, the associated noise with respect to each node is modeled as follows:

$$\eta_s^{t^{(1)}} \sim \mathcal{CN}(0, P_s {k_s^t}^2), \tag{1}$$

$$\eta_J^{t^{(1)}} \sim \mathcal{CN}(0, P_{J_1} {k_{J_1}^t}^2), \tag{2}$$

$$\eta_s^{t^{(2)}} \sim \mathcal{CN}(0, P_{J_2} {k_s^t}^2), \tag{3}$$

$$\eta_D^r \sim \mathcal{CN}(0, {k_D^r}^2 \sum_{i=1}^{N-1} P_{R_i} |g_{R_i}|^2), \tag{4}$$

$$\boldsymbol{\eta}_{R_{-1}}^r \sim \mathcal{CN}\left(0, {k_R^r}^2 \mathbf{\Pi}\left(P_s, P_{J_1}\right)\right), \tag{5}$$

$$\boldsymbol{\eta}_{R_{-1}}^t \sim \mathcal{CN}\left(0, {k_R^t}^2 \mathbf{\Lambda}\left(\boldsymbol{P}_{R_{-1}}\right)\right), \tag{6}$$

where

$$\mathbf{\Lambda}\left(\boldsymbol{P}_{R_{-1}}\right) \triangleq \mathrm{diag}(\boldsymbol{P}_{R_{-1}}),$$

$$\mathbf{\Pi}\left(P_s, P_{J_1}\right) \triangleq \mathrm{diag}\left[\left(P_s|f_{R1}|^2 + P_{J_1}|h_{R1}|^2\right), \ldots, \left(P_s|f_{R_{N-1}}|^2 + P_{J_1}|h_{R_{N-1}}|^2\right)\right],$$

and the parameters k_i^t and k_i^r for $i \in \{S, R_l \forall l \in L, D\}$, represent error vector magnitudes (EVM) [26], which characterize the level of impairments in the transmitter and receiver hardware, respectively. This quality parameter is defined as the ratio of the average impairment amplitude to the average signal amplitude. Notably, the EVM measures the joint influence of different HIs and compensation algorithms. Therefore, it can be measured directly in practice [26], [30], e.g., 3GPP LTE has an EVM requirement in the range of $k_i^t, k_i^r \in [0.08, 0.175]$ and naturally, for obtaining higher spectral efficiencies, we require hardware resulting in lower EVM values.

B. Signal Representation

We assume that the node J_1 chosen from $\boldsymbol{R}$, broadcasts the unit-power jamming $z^{(1)}$ to secure the concurrent transmission of the desired signal. Consequently, when considering the overall influence of HIs [27], [30], the signal vector received by the $N-1$ other untrusted relays, namely $\mathbf{y}_{\boldsymbol{R}_{-1}} \in \mathbb{C}^{(N-1)\times 1)}$ and by $\boldsymbol{E}$, i.e., $\boldsymbol{y}_E^{(1)} \in \mathbb{C}^{(N_E\times 1)}$ can be expressed as

$$\mathbf{y}_{R_{-1}} = \left(\sqrt{P_s}x_s + {\eta_s^t}^{(1)}\right)\mathbf{f}_{R_{-1}} + \left(\sqrt{P_{J_1}}z^{(1)} + {\eta_J^t}^{(1)}\right)\mathbf{h}_{R_{-1}} + \boldsymbol{\eta}_{R_{-1}}^r + \mathbf{n}_{R_{-1}}, \quad (7)$$

$$\mathbf{y}_E^{(1)} = \left(\sqrt{P_s}x_s + {\eta_s^t}^{(1)}\right)\mathbf{f}_E + \left(\sqrt{P_{J_1}}z^{(1)} + \eta_J^t\right)\mathbf{q}_E + \mathbf{n}_E^{(1)}, \quad (8)$$

where

- $\mathbf{f}_{R_{-1}} \triangleq [f_{R,1},\ f_{R,2},\ \ldots,\ f_{R,N-1}]^T$ and $\mathbf{h}_{R_{-1}} \triangleq [h_{R,1},\ h_{R,2},\ \ldots,\ h_{R,N-1}]^T$ represent the complex-valued channel coefficients from of the $S \rightarrow R_l$ and $J_1 \rightarrow R_l$, $\forall l \in \mathcal{L}$, respectively.
- $\mathbf{f}_E \in \mathbb{C}^{N_E\times 1}$and $\mathbf{q}_E \in \mathbb{C}^{N_E\times 1}$ denote the complex-valued channel coefficients of the $S \rightarrow E$ and $J_1 \rightarrow E$ lines, respectively.
- x_s is the transmitted signal by S with $\mathbb{E}\left\{|x_s|^2\right\} = 1$.
- Vector $\mathbf{n}_{R_{-1}} \triangleq [n_{R,1},\ n_{R,2},\ \ldots,\ n_{R,N-1}]^T \in \mathbb{C}^{(N-1)\times 1}$ with $\mathbf{n}_{R_{-1}} \sim \mathcal{CN}(0, \sigma^2\mathbf{I}_{N-1})$ representing the additive white Gaussian noise (AWGN) at $\boldsymbol{R}_{-1}$ and $\mathbf{n}_E^{(1)} \in \mathbb{C}^{N_E\times 1}$with $\mathbf{n}_E^{(1)} \sim \mathcal{CN}(0, \sigma^2\mathbf{I}_{N_E})$ representing the AWGN at E in phase I.

In phase II, the nodes in the set $\boldsymbol{R}_{-1}$ retransmits their received signal to D, which provides another opportunity for E to extract the confidential information. As mentioned before, in order to safeguard this phase,J_2 is employed. However, since the no information is available about E, the strategy to further protect the information from E, is to concurrently inject AN along with the information bearing signal forwarded by the relay nodes. Therefore, the signal transmitted by the set $\boldsymbol{R}_{-1}$ in the second phase is

$$\mathbf{x}_{R_{-1}} = \mathbf{W}^H\mathbf{y}_{R_{-1}} + \mathbf{n}_a, \quad (9)$$

where $\mathbf{n}_a \in \mathbb{C}^{(N-1)\times 1}$ is the AN vector with power $\boldsymbol{P}_{\mathrm{n}_a} \triangleq \left[P_{\mathrm{n}_{a,1}},\ P_{\mathrm{n}_{a,2}},\ \ldots,\ P_{\mathrm{n}_{a,N-1}}\right]^T \in \mathbb{R}^{(N-1)\times 1}$ and $P_{\mathrm{n}_{a,l}}$ therein denotes the power consumed by R_l, $\forall l \in \mathcal{L}$, while emitting AN. Still referring to (9) matrix $\mathbf{W}$ is the weight matrix in the form of $\mathbf{W}^H \triangleq \mathrm{diag}\left\{\boldsymbol{w}^*\right\}$, with beamformer vector obeying $\boldsymbol{w} \triangleq [w_1, w_2, \ldots, w_{N-1}]^T \in \mathbb{C}^{(N-1)\times 1}$ and w_l, $\forall l \in \mathcal{L}$ therein denotes the beamforming weight adopted by the lth relay. We assume $\|\boldsymbol{w}\|^2 = 1$ [17]. Note that, $\mathbf{x}_{R_{-1}}$ should satisfy both the individual power constraint at each relay and the total power constraint of the whole network as follows:

$$P_{R_l} = \mathbb{E}\left\{\left|x_{R_{-1},l}\right|^2\right\} \leq Q_l, \forall l \in \mathcal{L}, \quad (10)$$

$$P_{tot} = P_{R,tot} + P_s + P_{J_1} + P_{J_2} \leq Q_{tot}, \quad (11)$$

where $P_{R,tot}$ is the total power consumed by all the relay nodes in the set $\boldsymbol{R}_{-1}$, i.e., $P_{R,tot} = \mathbb{E}\left\{\mathbf{x}_{R_{-1}}^H\mathbf{x}_{R_{-1}}\right\} = \sum_{l=1}^{N-1}\mathbb{E}\left\{\left|x_{R_{-1},l}\right|^2\right\}$, Q_l is the transmit power budget of the lth relay node due to the hardware constraint, and Q_{tot} is the total power constraint of the entire network due to the associated spectrum mask constraint. As mentioned before, besides emitting AN by the set $\boldsymbol{R}_{-1}$, the node J_2 is configured to concurrently emit jamming signal. In this regard, if FACJ (i.e., $J_2 \in \boldsymbol{R}$) is deployed to confuse the Eve, the jamming AN $z^{(2)}$ will inevitably interfere with D. Hence, SACJ is the best choice for confusing the Eve. Indeed, since S is idle in phase II and there is no straight path between S and D, the pure jamming signal emitted by S is not received at D. Moreover, using S as a jammer, the remaining relay nodes can be exploited to provide an improved array gain. Hence, the average amount of information rate delivered to the legitimate terminal is increased. Accordingly, by configuring S to play the role of J_2, the received signals received at D and E are respectively, given by

$$y_{\mathrm{D}} = \mathbf{g}_{R_{-1}}^T\left(\mathbf{x}_{R_{-1}} + \boldsymbol{\eta}_{R_{-1}}^t\right) + \eta_D^r + n_D$$
$$= \sqrt{P_s}\mathbf{g}_{R_{-1}}^T\mathbf{W}^H\mathbf{f}_{R_{-1}}x_{_s} + \sqrt{P_{J_1}}\mathbf{g}_{R_{-1}}^T\mathbf{W}^H\mathbf{h}_{R_{-1}}z^{(1)} + \overline{n}_D, \quad (12)$$

$$\mathbf{y}_E^{(2)} = \mathbf{C}_E\left(\mathbf{x}_{R_{-1}} + \boldsymbol{\eta}_{R_{-1}}^t\right) + \left(\sqrt{P_{J_2}}z^{(2)} + {\eta_s^t}^{(2)}\right)\mathbf{f}_E + \mathbf{n}_E^{(2)}$$
$$= \sqrt{P_s}\mathbf{C}_E\mathbf{W}^H\mathbf{f}_{R_{-1}}x_{_s} + \sqrt{P_{J_1}}\mathbf{C}_E\mathbf{W}^H\mathbf{h}_{R_{-1}}z^{(1)} + \overline{\mathbf{n}}_E^{(2)}, \quad (13)$$

where

- $\mathbf{C}_E \in \mathbb{C}^{N_E\times(N-1)}$ whose lth column $\mathbf{c}_{E,l} \in \mathbb{C}^{N_E\times 1}$ specifies the complex-valued channel coefficient of the-from $R_l \rightarrow E$ line, $\forall l \in \mathcal{L}$ and vector $\mathbf{g}_{R_{-1}} \triangleq [g_{R,1},\ g_{R,2},\ \ldots,\ g_{R,N-1}]^T \in \mathbb{C}^{(N-1)\times 1}$, with $g_{R,l}$ denoting thees complex complex-valued channel coefficient of the $R_l \rightarrow D$, $\forall l \in \mathcal{L}$.
- $z^{(2)}$ is the jamming AN in phase II with $\mathbb{E}\left\{\left|z^{(2)}\right|^2\right\} = 1$.
- $n_D \sim \mathcal{CN}(0, \sigma^2)$ specifies the AWGN at D and $\mathbf{n}_E^{(2)} \in \mathbb{C}^{N_E\times 1}$ with $\mathbf{n}_E^{(2)} \sim \mathcal{CN}(0, \sigma^2\mathbf{I}_{N_E})$ represents the AWGN at E in phase II.
- $\overline{n}_D \triangleq \mathbf{g}_{R_{-1}}^T\mathbf{W}^H\mathbf{f}_{R_{-1}}{\eta_s^t}^{(1)} + \mathbf{g}_{R_{-1}}^T\mathbf{W}^H\mathbf{h}_{R_{-1}}{\eta_J^t}^{(1)} + \mathbf{g}_{R_{-1}}^T\mathbf{W}^H\boldsymbol{\eta}_{R_{-1}}^r + \mathbf{g}_{R_{-1}}^T\mathbf{W}^H\mathbf{n}_{R_{-1}} + \mathbf{g}_{R_{-1}}^T\boldsymbol{\eta}_{R_{-1}}^t + \mathbf{g}_{R_{-1}}^T\mathbf{n}_a + \eta_D^r + n_D$, and $\overline{\mathbf{n}}_E^{(2)} \triangleq \sqrt{P_{J_2}}\mathbf{f}_E z^{(2)} + \mathbf{C}_E\mathbf{W}^H\mathbf{f}_{R_{-1}}{\eta_s^t}^{(1)} + \mathbf{C}_E\mathbf{W}^H\mathbf{h}_{R_{-1}}{\eta_J^t}^{(1)} + {\eta_s^t}^{(2)}\mathbf{f}_E + \mathbf{C}_E\mathbf{W}^H\boldsymbol{\eta}_{R_{-1}}^r + \mathbf{C}_E\mathbf{W}^H\mathbf{n}_{R_{-1}} + \mathbf{C}_E\boldsymbol{\eta}_{R_{-1}}^t + \mathbf{C}_E\mathbf{n}_a + \mathbf{n}_E^{(2)}$.

Note that the AN emitted by the cooperative relays should be designed to fall in the null space of the legitimate terminal's channel, i.e., we consider the null space beamforming (NSB) technique of CJ. In other words, in the NSB technique, $\mathbf{n}_a$ can be considered in the form of $\mathbf{n}_a$=$\mathbf{U}\mathbf{z}$, where $\mathbf{U} \in \mathbb{C}^{(N-1)\times(N-2)}$ represents the orthonormal basis matrix related to the null space of $\mathbf{g}_{R_{-1}}$, where each column of $\mathbf{U}$ is orthogonal to $\mathbf{g}_{R_{-1}}^T$ so that we have $\mathbf{g}_{R_{-1}}^T\mathbf{n}_a$= 0, and the components of $\mathbf{z} \triangleq [z_1,\ z_2,\ \ldots,\ z_{N-2}]^T$ with $\mathbf{z} \sim \mathcal{CN}(0, \boldsymbol{\Xi})$

and $\boldsymbol{\Xi} \triangleq \operatorname{diag}\left([\sigma_{z,1}^2, \sigma_{z,2}^2, \ldots, \sigma_{z,N-2}^2]\right)$, should satisfy the individual power constraint of each relay in the set $\boldsymbol{R}_{-1}$.

Remark 1. It should be pointed out that, in the case of using the DACJ policy, the entire set of N relays participate in the relaying operation. If the intended receiver knows both the beamforming vector and the reciprocal CSIs of its channel to the relays, it can decode the source information with the aid of self-interference neutralization [12] without the need for designing the beamformer for nulling the jamming AN $z^{(1)}$ at the destination. In this case, the cooperative beamforming design at the relays benefits from increased degrees of freedom for further increasing the secrecy rate. Even though, in this work, we have also assumed this approach in our hybrid jamming scheme, due to lack of enough knowledge about the associated channel to relays and the weighted coefficients in practice, the self-interference cannot be readily removed, in practice. In these situations, an alternative solution is to appropriately designing the beamformer to eliminate the interfering signal at the destination [21].

To simplify the following calculations, we can express (12) after some manipulations and applying $\mathbf{g}_{R_{-1}}^T \mathbf{n}_a = 0$ as follows:

$$y_{\mathrm{D}} = \sqrt{P_s}\boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{f}_{R_{-1}} x_s + \sqrt{P_{J_1}} \boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} z^{(1)} + \tilde{n}_D, \tag{14}$$

with $\tilde{n}_D \triangleq \boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{f}_{R_{-1}} \eta_s^{t\,(1)} + \boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} \eta_J^{t\,(1)} + \boldsymbol{w}^H \mathbf{G}_{R_{-1}} \boldsymbol{\eta}_{R_{-1}}^r + \boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{n}_{R_{-1}} + \mathbf{g}_{R_{-1}}^T \boldsymbol{\eta}_{R_{-1}}^t + \eta_D^r + n_D$ and $\mathbf{G}_{R_{-1}} \triangleq \operatorname{diag}(\mathbf{g}_{R_{-1}})$. On the other hand, since E has two opportunities to wiretap the information, the optimal strategy adopted by E is to combine the information received from the transmissions of both S and $\boldsymbol{R}_{-1}$ during two phases. Therefore, combining (8) and (13) yields the receiver model of E in the consecutive transmission phases as

$$\mathbf{y}_{\mathrm{E}} = \mathbf{H}_E x_s + \mathbf{n}_E, \tag{15}$$

where we have

$$\mathbf{H}_E = \begin{bmatrix} \sqrt{P_s}\mathbf{f}_E \\ \sqrt{P_s}\mathbf{C}_E \mathbf{F}_{R_{-1}} \boldsymbol{w}^* \end{bmatrix},$$

$$\mathbf{n}_E = \begin{bmatrix} \overline{\mathbf{n}}_E^{(1)} \\ \sqrt{P_{J_1}} \mathbf{C}_E \mathbf{H}_{R_{-1}} \boldsymbol{w}^* z^{(1)} + \overline{\mathbf{n}}_E^{(2)} \end{bmatrix}, \tag{16}$$

with $\mathbf{F}_{R_{-1}} \triangleq \operatorname{diag}(\mathbf{f}_{R_{-1}})$, $\mathbf{H}_{R_{-1}} \triangleq \operatorname{diag}(\mathbf{h}_{R_{-1}})$, $\overline{\mathbf{n}}_E^{(1)} \triangleq \sqrt{P_{J_1}} \mathbf{q}_E z^{(1)} + \mathbf{f}_E \eta_s^{t\,(1)} + \mathbf{q}_E \eta_J^{t\,(1)} + \mathbf{n}_E^{(1)}$. Note that $\mathbf{n}_E$ is a zero-mean Gaussian vector having a covariance matrix of $\mathbf{Q}_E = \mathbb{E}\left\{\mathbf{n}_E \mathbf{n}_E^H\right\} \in \mathbb{C}^{2N_E \times 2N_E}$, which is given by

$$\mathbf{Q}_E = \begin{bmatrix} Q_{E_{11}} & Q_{E_{12}} \\ Q_{E_{21}} & Q_{E_{22}} \end{bmatrix}, \tag{17}$$

where, $Q_{E_{11}} = \tau_{J_1} P_{J_1} \mathbf{q}_E \mathbf{q}_E^H + P_s {k_s^t}^2 \mathbf{f}_E \mathbf{f}_E^H + \sigma^2 \boldsymbol{I}_{N_E}$, $Q_{E_{12}} = {k_{J_1}^t}^2 P_{J_1} \mathbf{q}_E \boldsymbol{w}^T \mathbf{H}_{R_{-1}}^H \mathbf{C}_E^H + P_s {k_s^t}^2 \mathbf{f}_E \boldsymbol{w}^T \mathbf{F}_{R_{-1}}^H \mathbf{C}_E^H$, $Q_{E_{21}} = \tau_{J_1} P_{J_1} \mathbf{C}_E \mathbf{H}_{R_{-1}} \boldsymbol{w}^* \mathbf{q}_E^H + P_s {k_s^t}^2 \mathbf{C}_E \mathbf{F}_{R_{-1}} \boldsymbol{w}^* \mathbf{f}_E^H$, $Q_{E_{22}} = {k_{J_1}^t}^2 P_{J_1} \mathbf{C}_E \mathbf{H}_{R_{-1}} \boldsymbol{w}^* \boldsymbol{w}^T \mathbf{H}_{R_{-1}}^H \mathbf{C}_E^H + P_{J_1} {k_R^r}^2 \mathbf{C}_E \mathbf{H}_{R_{-1}} \mathbf{W}^H \mathbf{W} \mathbf{H}_{R_{-1}}^H \mathbf{C}_E^H + \tau_s P_{J_2} \mathbf{f}_E \mathbf{f}_E^H + P_s {k_s^t}^2 \mathbf{C}_E \mathbf{F}_{R_{-1}} \boldsymbol{w}^* \boldsymbol{w}^T \mathbf{F}_{R_{-1}}^H \mathbf{C}_E^H + P_s {k_R^r}^2 \mathbf{C}_E \mathbf{F}_{R_{-1}} \mathbf{W}^H \mathbf{W} \mathbf{F}_{R_{-1}}^H \mathbf{C}_E^H + \sigma^2 \mathbf{C}_E \mathbf{W}^H \mathbf{W} \mathbf{C}_E^H + {k_R^t}^2 \mathbf{C}_E \boldsymbol{\Lambda}\left(\boldsymbol{P}_{R_{-1}}\right) \mathbf{C}_E^H + \mathbf{C}_E \mathbf{U} \boldsymbol{\Xi} \mathbf{U}^H \mathbf{C}_E^H + \sigma^2 \boldsymbol{I}_{N_E}$, and $\tau_s \triangleq 1 + {k_s^t}^2$.

III. Secrecy Scheme in the Presence of Untrusted Relays and a Passive Eavesdropper

Before proceeding this section we have provided a diagram, depicted in Fig. 3, to show the flow of the analysis described in the sequel. This diagram facilitates the legibility of this paper for the readers to know, what comes next in this long paper. The achievable maximum instantaneous secrecy rate under the existence presence of both E and the untrusted relays can be expressed as [11]-[13], [17]

$$R_s = \max\left[I\left(y_D; x_s\right) - \max_{i \in \{\boldsymbol{R}_{-1}, \boldsymbol{E}\}} I\left(y_i; x_s\right) \right]^+, \tag{18}$$

where $[a]^+ = \max(0,\ a)$, and $I(.;.)$ denotes the mutual information. In our problem, the legitimate destination D observes an equivalent single-input single-output (SISO) channel. Accordingly, by defining $\boldsymbol{\Phi}_{Gf} \triangleq \mathbf{G}_{R_{-1}} \mathbf{f}_{R_{-1}} \mathbf{f}_{R_{-1}}^H \mathbf{G}_{R_{-1}}^H$, $\boldsymbol{\Phi}_{Gh} \triangleq \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} \mathbf{h}_{R_{-1}}^H \mathbf{G}_{R_{-1}}^H$, $\boldsymbol{\Phi}_{GH} \triangleq \mathbf{G}_{R_{-1}}^H \mathbf{H}_{R_{-1}} \mathbf{H}_{R_{-1}}^H \mathbf{G}_{R_{-1}}$, $\boldsymbol{\Phi}_{GF} \triangleq \mathbf{G}_{R_{-1}} \mathbf{F}_{R_{-1}} \mathbf{F}_{R_{-1}}^H \mathbf{G}_{R_{-1}}^H$, $\boldsymbol{\Phi}_G \triangleq \mathbf{G}_{R_{-1}} \mathbf{G}_{R_{-1}}^H$, the information rate $I\left(y_D; x_s\right)$ achieved by the legitimate terminal is expressed in (19) at the top of next page where $\boldsymbol{\Psi}_k\left(P_s, P_{J_1}\right) \triangleq P_{J_1} \tau_{J_1} \boldsymbol{\Phi}_{Gh} + P_{J_1} {k_R^r}^2 \boldsymbol{\Phi}_{GH} + P_s {k_s^t}^2 \boldsymbol{\Phi}_{Gf} + P_s {k_R^r}^2 \boldsymbol{\Phi}_{GF} + \sigma^2 \boldsymbol{\Phi}_G$ and $\tau_{RD} \triangleq {k_R^t}^2 + {k_D^r}^2$, $\tau_{J_1} \triangleq 1 + {k_{J_1}^t}^2$.

We also remark that, the untrusted relay in the set $\boldsymbol{R}_{-1}$ only has a single opportunity to capture the information. As such, if the measured SINR at R_l in the presence of the jammer node J_1 is by $\Omega_l^{J_1}$ and h_{l-J_1} denotes represents the channel coefficient between the lth relay and jammer J_1, the information leakage at the lth untrusted relay node denoted by $I\left(y_{R_l}; x_s\right)$ is formulated as follows:

$$I\left(y_{R_l}; x_s\right) = \frac{1}{2}\log_2\left(1 + \Omega_l^{J_1}\right), \tag{20}$$

where, $\Omega_l^{J_1} \triangleq \frac{P_s |\mathrm{f}_{Rl}|^2}{P_{J_1} \tau_{RJ_1} \left|h_{l-J_1}\right|^2 + P_s \tau_{RS} |f_{Rl}|^2 + \sigma^2}$, $\tau_{RS} \triangleq {k_s^t}^2 + {k_R^r}^2$ and $\tau_{RJ_1} \triangleq \tau_{J_1} + {k_R^r}^2$. Additionally, the rate of the information leaked to the E can be quantified by the sum rate of the multi-input multi-output (MIMO) system in (15) which is given by

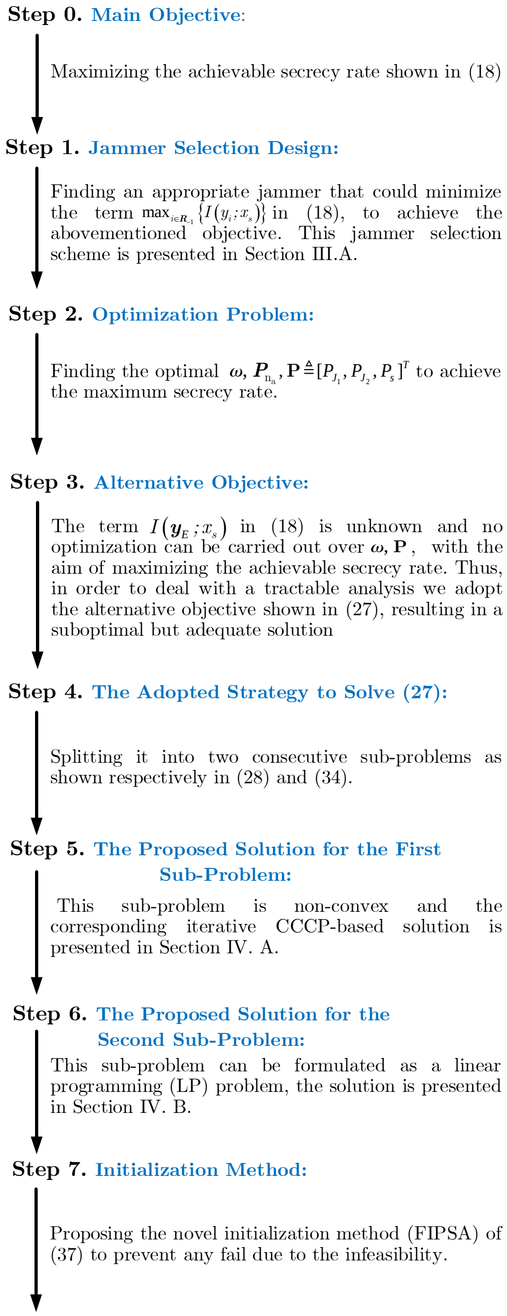
$$I\left(y_E; x_s\right) = \frac{1}{2}\log_2\left(\det\left(\mathbf{I}_{2N_E} + \mathbf{H}_E \mathbf{H}_E^H \boldsymbol{Q}_E^{-1}\right)\right), \tag{21}$$

In general, we hope to achieve the maximum secrecy rate by finding the optimal $\boldsymbol{w}$, $\boldsymbol{P}_{\mathrm{n}_a}$, $\mathbf{P} \triangleq [\ P_{J_1}, P_{J_2},\ \ P_s]^T$ and selecting the optimal jammer $\overset{\circ}{J}$. To achieve this objective, in the sequel, we first focus our attention on the jammer selection design. Then we describe the proposed joint optimal power allocation and cooperative AN-aided beamforming (OPA-CANB) scheme involved for providing PLS in our network.

A. Suboptimal Jammer Selection

Upon assuming that the perfect CSI of Eve is known at S, it was shown in [17] that the optimal jammer node $\overset{\circ}{J_1}$ can be found by identifying the most curious node in the set of untrusted relays and the detected eavesdropper phase II of the solution proposed in [17], the NSB technique was exploited at the relay nodes, leading to completely eliminating the information leakage at E, because the NSB technique

$$I\left(y_D; x_s\right) = \frac{1}{2}\log_2\left(1 + \frac{P_s \boldsymbol{w}^H \boldsymbol{\Phi}_{Gf} \boldsymbol{w}}{\boldsymbol{w}^H \boldsymbol{\Psi}_k\left(P_s, P_{J_1}\right)\boldsymbol{w} + \tau_{RD}\mathbf{g}_{R_{-1}}^T \boldsymbol{\Lambda}\left(\boldsymbol{P}_{R_{-1}}\right)\mathbf{g}_{R_{-1}}^* + \sigma^2}\right) \tag{19}$$


Step 0. Main Objective:

Maximizing the achievable secrecy rate shown in (18)

Step 1. Jammer Selection Design:

Finding an appropriate jammer that could minimize the term $\max_{i\in\boldsymbol{R}_{-1}}\left\{I\left(y_i; x_s\right)\right\}$ in (18), to achieve the abovementioned objective. This jammer selection scheme is presented in Section III.A.

Step 2. Optimization Problem:

Finding the optimal $\boldsymbol{\omega}$, $\boldsymbol{P}_{\mathrm{n_a}}$, $\mathbf{P} \triangleq [P_{J_1}, P_{J_2}, P_s]^T$ to achieve the maximum secrecy rate.

Step 3. Alternative Objective:

The term $I\left(\boldsymbol{y}_E; x_s\right)$ in (18) is unknown and no optimization can be carried out over $\boldsymbol{\omega}$, $\mathbf{P}$, with the aim of maximizing the achievable secrecy rate. Thus, in order to deal with a tractable analysis we adopt the alternative objective shown in (27), resulting in a suboptimal but adequate solution

Step 4. The Adopted Strategy to Solve (27):

Splitting it into two consecutive sub-problems as shown respectively in (28) and (34).

Step 5. The Proposed Solution for the First Sub-Problem:

This sub-problem is non-convex and the corresponding iterative CCCP-based solution is presented in Section IV. A.

Step 6. The Proposed Solution for the Second Sub-Problem:

This sub-problem can be formulated as a linear programming (LP) problem, the solution is presented in Section IV. B.

Step 7. Initialization Method:

Proposing the novel initialization method (FIPSA) of (37) to prevent any fail due to the infeasibility.

Fig. 3. Flow of the mathematical analysis

facilitated the specific design of $\boldsymbol{w}$ for ensuring that the info leakage falls in the null space of the equivalent channel of the relay link spanning from S to the E. Thus there is no need for the jammer in the second phase. By contrast, in this paper, E is entirely passive, hence the beamforming vector cannot be designed for eliminating the information leakage. Furthermore, given that the CSI of E is unknown, we cannot calculate $I\left(y_E; x_s\right)$ in (21), hence we can not consider node E for jammer selection anymore, which results in a suboptimal but adequate solution.

Based on the preceding discussions, in our scenario the suboptimal jammer node J_1° can be obtained based on the ability of each node to reduce the received SINR at the most curious node among the untrusted relays only. Additionally, as mentioned earlier, in phase II we harness the silent node S as J_2° to assist the AN generation by the relay set for further confusing the potential Eve.

Now, in order to determine J_1°, we first calculate Ω_l^j denoting the measured SINR at the R_l in the presence of a randomly selected jammer candidate $j \in \{\boldsymbol{R}, D\}$, which is given by

$$\Omega_l^j = \frac{P_s |f_{Rl}|^2}{P_{J_1}\tau_{Rj}|h_{l-j}|^2 + P_s\tau_{RS}|f_{Rl}|^2 + \sigma^2}, \tag{22}$$

where the definitions of τ_{Rj} and h_{l-j} are the same as in (20). The metric (22) is evaluated for $\forall j \in \{\boldsymbol{R}, D\}$ at each $l \in \{\boldsymbol{R} \mid l \neq j\}$, separately. Accordingly, assuming that the node $j \in \{\boldsymbol{R}, D\}$ is a jammer candidate, we can readily find the specific R_{l*}^j at which the highest amount of information is leaked in comparison to all the other untrusted relay nodes (i.e., the node R_{l*}^j has received the highest SINR values Ω_{l*}^j in the presence of the jammer candidate j). Mathematically, this can be expressed as

$$\left[\Omega_{l*}^j, R_{l*}^j\right] = \begin{cases} \underset{l}{max}\left\{\boldsymbol{S}_1\right\} & ; j = D \\ \underset{l}{max}\left\{\boldsymbol{S}_2\right\} & ; j \in \boldsymbol{R} \end{cases}, \tag{23}$$

where, $\boldsymbol{S}_1 \triangleq \left\{\Omega_1^j,\ \Omega_2^j,\ \ldots,\ \Omega_N^j\right\}$ and $\boldsymbol{S}_2 \triangleq \left\{\Omega_1^j,\ \Omega_2^j,\ \ldots, \Omega_{j-1}^j, \Omega_{j+1}^j, \ldots,\ \Omega_N^j\right\}$. Now by finding the specific node R_{l*}^j as the node suffering from the highest information leakage, we have to see which jammer candidate $j \in \{\boldsymbol{R}, D\}$ could better protect the confidential data from being intercepted by R_{l*}^j. To do so, we have to find the minimum value among the measured Ω_{l*}^j values, yielding the suboptimal jammer J_1°, which prevents the most curious relay node $R_{l^{\circ}}^{J_1^{\circ}}$ from capturing the information signal. Accordingly, the suboptimal jammer J_1° is found by

$$\left[J_1^{\circ}, R_{l^{\circ}}^{J_1^{\circ}}\right] = \min_{j\epsilon\{\boldsymbol{R}, D\}}\left\{\Omega_{l*}^j\right\}, \tag{24}$$

It is worth mentioning that, dedicating more relays to cooperative jamming in phase I has the benefit of better confusing the passive Eve. However, this leads to reducing the number of active relays in phase II, which potentially degrades the legitimate channel. Furthermore, we should point out that thanks to the known CSI of the link spanning from $\boldsymbol{R}_{-1}$ to D, the relay nodes are capable of determining $\boldsymbol{w}$ in order to null out $\mathbf{n}_a$ emitted by the set $\boldsymbol{R}_{-1}$ at D via the NSB technique. Hence, if less relay nodes are invoked for CB inat phase II, a lower degrees of freedom is provided for performing NSB. Based on what was discussed above, we prefer to choose only a single jammer from relays.

Remark 2. Although P_s and P_{J_1} are optimization variables, the values of these variables are not specified at the jammer selection stage. Therefore, it is recommended to use the following values to select the appropriate jammer. Accordingly, assuming while S broadcasts its data with its maximum power constraint, i.e., $P_s = P_T$, together with the fact that (22) is a strictly decreasing functions with respect to P_{J_1}, in order to keep the information leaked towards the curious nodes as small as possible we have let $P_{J_1} = \overline{P}_{J_1}$. We will see in the simulation results that these choices are appropriate for suboptimum jammer selection.

B. Joint OPA-CANB Design

By finding both J_1° and $R_{l^\circ}^{J_1^\circ}$, the maximization problem in (18) is simplified to a certain degree, but substituting into (18) results in a nonlinear and non-convex function of both $\boldsymbol{w}$ and $\mathbf{P}$ for the achievable secrecy rate. Accordingly, we deal with an intractable joint optimization problem. On the other hand, since the CSIs correspond to E given by $\mathbf{f}_E$, $\mathbf{q}_E$ and $\mathbf{c}_E$ are all unknown in our network, we cannot carry out any optimization over $\boldsymbol{w}$, $\mathbf{P}$ with the aim of maximizing the achievable secrecy rate. Generally speaking, finding a global optimum for the above mentioned non-convex secrecy rate maximization problem is computationally expensive or may even become intractable. Hence we have to find a way forward for more tractable analysis. In this regard, by scrutinizing the overall allocated power to the network in (11), we discover that it can be divided into two portions. The first portion comprises the power assigned to convey the information signal, while the second portion is dedicated for confusing the curious nodes. As such, a possible way of striking a tradeoff between the security and reliability is to optimally distribute the power between these two part. Proceeding along this line, we first rewrite the total power consumed by the set $\boldsymbol{R}_{-1}$ in the form of $P_{R,tot} = P_I + P_{AN}$, where we have $P_I \triangleq \boldsymbol{w}^H \boldsymbol{\Upsilon}_k \left(P_s\ , P_{J_1}\right) \boldsymbol{w}$ with $\boldsymbol{\Upsilon}_k \left(P_s\ , P_{J_1}\right) \triangleq P_s \left(1+\tau_{RS}\right) \mathbf{F}_{R_{-1}} \mathbf{F}_{R_{-1}}^H + P_{J_1} \tau_{RJ_1} \mathbf{H}_{R_{-1}} \mathbf{H}_{R_{-1}}^H + \sigma^2 \mathbf{I}_{N-1}$, as the power consumed to convey the desired information, and $P_{AN} \triangleq \mathbb{E}\left\{\mathbf{n}_a^H \mathbf{n}_a\right\} = \sum_{k=1}^{N-1} P_{\mathrm{n}_{a,k}} = \sum_{k=1}^{N-2} \sigma_{z,k}^2$ denotes the total power allocated to the AN $\mathbf{n}_a$. Thus, based on the preceding discussions, while the power allocated for conveying the information-bearing part in both phases $P_I + P_s$ should be capable of maintaining the minimum reliability requirement at the legitimate terminal D the remaining power assigned to the AN have to be shared among relay nodes such that confusing P_{AN} is maximized for the E, as much as possible. It should also be pointed out that, although we possess no knowledge about the passive Eve, the untrusted relays' CSI is perfectly known at the transmitter. Therefore, to reduce the information leakage at the untrusted relays during the first phase, we should also minimize the SINR at the most curious relay node.

It should also be pointed out that the jamming signal $z^{(1)}$ is unknown to D. However, this interfering signal has been forwarded to D by the set $\boldsymbol{R}_{-1}$ in phase II. As a countermeasure, the NSB should be adopted at $\boldsymbol{R}_{-1}$ for eliminating the jamming signal $z^{(1)}$ at the intended receiver, which facilitates the joint design about to be described in the following, By doing so, the beamforming vector $\boldsymbol{w}$ should be adjusted for ensuring that $z^{(1)}$ lies within the null-space of the equivalent channel of the relay link between S and D, i.e., we have $\boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} = 0$. In other words, $\boldsymbol{w}$ is considered to be in the form of $\boldsymbol{w} = \mathbf{H}\boldsymbol{v}$, where $\mathbf{H} \in \mathbb{C}^{(N-1)\times(N-2)}$ is the column-orthogonal projection matrix that projects $\boldsymbol{w}$ onto the null space of the matrix $\mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}}$, i.e., we have $\mathbf{H}^H \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} {=} 0$, and $\boldsymbol{v} \in \mathbb{C}^{(N-1)\times 1}$ is an arbitrary vector which should be optimized.

Now, given $\boldsymbol{\Lambda}(\boldsymbol{P}_{R_{-1}}) = \boldsymbol{\Lambda}\left(\boldsymbol{P}_{\mathrm{n}_a}\right) + \mathbf{W}^H \boldsymbol{\Upsilon}_k \left(P_s\ , P_{J_1}\right) \mathbf{W}$, with $\boldsymbol{\Lambda}\left(\boldsymbol{P}_{\mathrm{n}_a}\right) \triangleq \mathrm{diag}(\boldsymbol{P}_{\mathrm{n}_a})$, which represents the power consumed by each relay in phase II in a matrix form, and also exploiting $\boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} = 0$ based on the NSB condition described above, $I\left(y_D; x_s\right)$ in (17) can be rewritten after some manipulations can be rewritten as (25) shown at top of next page, where we have $\widetilde{\boldsymbol{\Psi}}_k\left(P_s, P_{J_1}\right) {\triangleq} P_{J_1} k_1 \boldsymbol{\Phi}_{GH} + P_s k_2 \boldsymbol{\Phi}_{GF} + P_s {k_s^t}^2 \boldsymbol{\Phi}_{Gf} + \sigma^2 k_3 \boldsymbol{\Phi}_G$ with $k_1 \triangleq \tau_{RD}\tau_{RJ_1} + {k_R^r}^2$, $k_2 \triangleq \tau_{RD}\left(1+\tau_{RS}\right) + {k_R^r}^2$ and $k_3 \triangleq 1 + \tau_{RD}$. On the other hand, by plugging substituting $\boldsymbol{\Lambda}\left(\boldsymbol{P}_{\mathrm{n}_a}\right) \triangleq \mathbb{E}\left\{\mathbf{n}_a \mathbf{n}_a^H\right\}$ into (23) together with considering $\mathbf{g}_{R_{-1}}^T \mathbf{n}_a {=}\ 0$, as discussed earlier, $I\left(y_D; x_s\right)$ becomes

$$I\left(y_D; x_s\right) = \frac{1}{2}\log_2\left(1 + \frac{P_s \boldsymbol{w}^H \boldsymbol{\Phi}_{Gf} \boldsymbol{w}}{\boldsymbol{w}^H \widetilde{\boldsymbol{\Psi}}_k\left(P_s, P_{J_1}\right) \boldsymbol{w} + \sigma^2}\right), \tag{26}$$

We also note that, the security in phase II depends on not only the AN level imposed by the relay nodes, but also related to the jamming power emitted by J_2. Although it seems better for J_2 to inject jamming at its maximum power, due to the limited power budget of the whole network, it is preferred to acquire the optimized value of this power, as well.

IV. Problem Formulation

Based on the above discussions, our objective is to: a) minimize the power allocated for transmitting the desired information during the two phases while maintaining the minimum QoS and, b) maximize the total power of $\mathbf{n}_a$ and $z^{(2)}$ to improve the security of the system. To realize these aims, the beamforming vector $\boldsymbol{w}$, the power $P_{\mathrm{n}_{a,l}}$ consumed by R_l, $\forall l \in \mathcal{L}$ to transmit the AN, and the power vector $\mathbf{P}$ should be jointly optimized under the following conditions:

1) NSB condition: $\boldsymbol{w}^H \mathbf{G}_{R_{-1}} \mathbf{h}_{R_{-1}} = 0$ or equivalently $\boldsymbol{w} = \mathbf{H}\boldsymbol{v}$. It should be noted that, as can be observed from (26), although this design of $\boldsymbol{w}$ nulls out $z^{(1)}$ at D, based on the implicit argument $P_{J_1} k_1 \boldsymbol{\Phi}_{GH}$ within $\widetilde{\boldsymbol{\Psi}}_k\left(P_s, P_{J_1}\right)$, we conclude that interference still remains at D, which degrades the overall secrecy performance and cannot be readily eliminated.
2) The SINR at the input of the legitimate terminal D should be above a predefined threshold γ.
3) The SINR denoted by $\Omega_{l^*}^{J1}$ and experienced by the most curious untrusted relay, during the first phase should be

$$I\left(y_D;x_s\right)=\frac{1}{2}\log_2\left(1+\frac{P_s\boldsymbol{w}^H\boldsymbol{\Phi}_{Gf}\boldsymbol{w}}{\boldsymbol{w}^H\widetilde{\boldsymbol{\Psi}}_k\left(P_s,P_{J_1}\right)\boldsymbol{w}+\tau_{RD}\mathbf{g}_{R_{-1}}^T\boldsymbol{\Lambda}\left(\boldsymbol{P}_{\mathrm{n}_a}\right)\mathbf{g}_{R_{-1}}^{*}+\sigma^2}\right), \tag{25}$$

minimized. In order to realize this ambitious objective, we incorporate a dynamic slack variable μ into the so-obtained cost function which can be regarded as an upper bound for the SINR at the most curious untrusted relay. This variable should be minimized and it is updated at each iteration based on the values of P_s and P_{J_1} obtained in the previous iteration, although we note that its minimization is not the main objective of our algorithm.

4) The signal forwarded via $\boldsymbol{R}_{-1}$ should satisfy both the individual power constraint of each relay node (Eq. (10)) and the total power constraint of the entire network (Eq. (11)).

By taking all of these into consideration, our optimization problem can be formulated as a max-min problem as follows:

$$\mathbf{P}_0:\max_{\sigma_{z,k}^2,P_{J_2}}\Bigg[\Bigg\{\min_{P_s,P_{J_1},\boldsymbol{v}}\Big[\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k\left(P_s\ ,P_{J_1}\right)\boldsymbol{v}$$

$$+P_s+\mu\Big]\Bigg\}+\mathbf{1}_{N-2}^T\boldsymbol{\sigma}+P_{J_2}\Bigg], \tag{27}$$

s.t.

$$\frac{P_s\boldsymbol{v}^H\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}}{\boldsymbol{v}^H\overline{\boldsymbol{\Psi}}_{\boldsymbol{k}}\left(P_s,P_{J_1}\right)\boldsymbol{v}+\sigma^2}\geq\gamma, \qquad (27-a)$$

$$\Omega_{l^*}^{J1}\leq\mu, \qquad (27-b)$$

$$\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k^{l,l}\left(P_s,P_{J_1}\ \right)\boldsymbol{v}+P_{\mathbf{n}_{a,l}}\leq Q_l\ ,\ \forall l\in\mathcal{L}, \qquad (27-c)$$

$$\mathbf{1}_3^T\mathbf{P}+\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k\left(P_s,P_{J_1}\ \right)\boldsymbol{v}+\mathbf{1}_{N-2}^T\boldsymbol{\sigma}\leq Q_{tot}, \qquad (27-d)$$

$$0<P_{J_1}\leq\overline{P}_{J_1}, \qquad (27-e)$$

$$0<P_{J_2}\leq\overline{P}_{J_2}, \qquad (27-f)$$

$$0<P_s\leq P_T. \qquad (27-g)$$

where, $\overline{\boldsymbol{\Upsilon}}_k\left(P_s\ ,P_{J_1}\right)\triangleq\mathbf{H}^H\boldsymbol{\Upsilon}_k\left(P_s\ ,P_{J_1}\right)\mathbf{H}$, $\overline{\boldsymbol{\Phi}}_{Gf}\triangleq\mathbf{H}^H\boldsymbol{\Phi}_{Gf}\mathbf{H}$, $\overline{\boldsymbol{\Psi}}_{\boldsymbol{k}}\left(P_s,P_{J_1}\right)\triangleq\mathbf{H}^H\widetilde{\boldsymbol{\Psi}}_{\boldsymbol{k}}\left(P_s,P_{J_1}\right)\mathbf{H}$, $\boldsymbol{\sigma}\triangleq\left[\sigma_{z,1}^2,\ \sigma_{z,2}^2,\ldots,\sigma_{z,N-2}^2\right]^T\in\mathbb{R}^{N-2}$, $\mathbf{1}_M\triangleq[1,\ 1,\ldots,1]^T\in\mathbb{R}^{\mathrm{M}}$, $\overline{\boldsymbol{\Upsilon}}_k^{l,l}\left(P_s,P_{J_1}\ \right)\triangleq P_s\left(1+\tau_{RS}\right)\mathbf{H}^H\mathbf{F}_{R_{-1}}\mathbf{e}_l\mathbf{e}_l^H\mathbf{F}_{R_{-1}}^H\mathbf{H}\ +P_{J_1}\tau_{RJ_1}\mathbf{H}^H\mathbf{H}_{R_{-1}}\mathbf{e}_l\mathbf{e}_l^H\mathbf{H}_{R_{-1}}^H\mathbf{H}+\sigma^2$and $\mathbf{e}_l$ therein is an unit vector, whose lth entry equals to one.

Let us now exploit that the max-min problem in (27), can be split into two consecutive sub-problems. Following this approach, in order to establish both secure and reliable communication, the term $\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k\left(P_s\ ,P_{J_1}\right)\boldsymbol{v}+P_s+\mu$, is firstly minimized over $\boldsymbol{v}$,P_s, and P_{J_1}. To arrive at a more tractable form of for (27) and to assign the minimum power to the information bearing part, we first assume that as much power as possible is allocated to convey the information bearing part, while no power is dedicated to the AN of the second phase, i.e., we have $P_{\mathbf{n}_{a,l}}=0$, $\forall l\in\mathcal{L}$ and $P_{J_2}=0$.

A. First Sub-Problem

Relying on what discussed above, by substituting the formula of $\Omega_{l^*}^{J1}$ into (27-b), and introducing the new power allocation vector $\overline{\mathbf{P}}\triangleq\left[\ P_{J_1},\ \ P_s\right]^T$ for ease of exposition, the first sub-problem can be expressed as the following minimization problem

$$\mathbf{P}_1:\min_{\overline{\mathbf{P}},\boldsymbol{v}}\mathcal{D}_k(\overline{\mathbf{P}},\boldsymbol{v})\triangleq\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k\left(\overline{\mathbf{P}}\right)\boldsymbol{v}+P_s+\mu, \tag{28}$$

s.t.

$$\frac{P_s\boldsymbol{v}^H\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}}{\boldsymbol{v}^H\overline{\boldsymbol{\Psi}}_{\boldsymbol{k}}\left(\overline{\mathbf{P}}\right)\boldsymbol{v}+\sigma^2}\geq\gamma, \qquad (28-a)$$

$$\frac{P_s\left|f_{R_l}\right|^2}{P_{J_1}\tau_{RJ_1}\left|h_{l^*-J_1}\right|^2+P_s\tau_{RS}\left|f_{R_l}\right|^2+\sigma^2}\leq\mu, \qquad (28-b)$$

$$\mathcal{D}_k^{l,l}(\overline{\mathbf{P}},\boldsymbol{v})\triangleq\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k^{l,l}\left(\overline{\mathbf{P}}\right)\boldsymbol{v}\leq Q_l\ ,\ \forall l\in\mathcal{L}, \qquad (28-c)$$

$$\mathbf{1}_2^T\overline{\mathbf{P}}+\mathcal{D}_k(\overline{\mathbf{P}},\boldsymbol{v})\leq Q_{tot}, \qquad (28-d)$$

$$0<P_{J_1}\leq\overline{P}_{J_1}, \qquad (28-e)$$

$$0<P_s\leq P_T. \qquad (28-f)$$

Remarkably, even with fixed $\overline{\mathbf{P}}$, the problem in (28) is still a non-convex quadratically constrained quadratic program (QCQP) with respect to the beamforming vector $\boldsymbol{v}$, which results in a computationally expensive or even intractable process for finding the global optimum. Therefore, designing an efficient algorithm for finding a local optimum of the non-convex problem in (28) is more preferable in practice. We now proceed, by exploiting a suitable transformation of variables and transform the optimization problem (28) into an equivalent DC[1] program [32]. To solve the resultant DC program, a low-complexity iterative algorithm is proposed, which is based on the constrained concave-convex procedure (CCCP) and yields a local optimum of the DC program, and subsequently a local optimum offor the problem (28), as well. Incidentally, the non-convex problem (28) is approximated through a sequence of convex problems that can be solved efficiently.

1) DC Program Re-Formulation of the $\mathbf{P_1}$*:* The multiplicative terms comprised of the variables $\boldsymbol{v}$, P_{J_1}, and P_s appeared in both the objective function and in the constraints, which is an obstacle of solving the optimization problem (28). To deal with this problem, the following variables transformation is introduced for arriving at a tractable problem formulation

$$q_{J_1}\triangleq\frac{1}{P_{J_1}},q_s\triangleq\frac{1}{P_s},\text{and }\mathbf{q}\triangleq\left[q_{J_1},\ \ q_s\right]^T, \tag{29}$$

[1] DC programs are optimization problems whose objective and/or constraint functions can be transformed into a difference of convex functions [31].

Explicitly by involving the variable transformation in (29), the problem in (28) is converted into a strictly convex function, while the SINR constraints in (28-a) and (28-b) are converted into inequality constraints of DC form [31], [32]. Subsequently, the DC program reformulation of $\mathbf{P}_1$ becomes

$$\mathbf{P}_2 : \min_{\mathbf{q},\boldsymbol{v}} \mathcal{D}_k(\mathbf{q},\boldsymbol{v}) \triangleq \boldsymbol{v}^H \overline{\boldsymbol{\Upsilon}}_k(\mathbf{q})\,\boldsymbol{v} \; + \frac{1}{q_s} + \mu, \qquad (30)$$

s.t.

$$\mathcal{T}_k(\mathbf{q},\boldsymbol{v}) \triangleq \boldsymbol{\beta}_k(\mathbf{q},\boldsymbol{v}) - \boldsymbol{\alpha}(\mathbf{q},\boldsymbol{v}) \le 0, \qquad (30-a)$$

$$\mho_k(\mathbf{q}) \triangleq \kappa(\mathbf{q},\mu) - \xi(q_s) \le 0, \qquad (30-b)$$

$$\mathcal{D}_k^{l,l}(\mathbf{q},\boldsymbol{v}) \triangleq \boldsymbol{v}^H \overline{\boldsymbol{\Upsilon}}_k^{l,l}(\mathbf{q})\,\boldsymbol{v} \le Q_l \;, \forall l \in \mathcal{L}, \qquad (30-c)$$

$$\mathbf{1}_2^T\mathbf{q} + \mathcal{D}_k(\mathbf{q},\boldsymbol{v}) \le Q_{tot}, \qquad (30-d)$$

$$\tfrac{1}{q_{J_1}} \le \overline{P}_{J_1}, \qquad (30-e)$$

$$\tfrac{1}{q_s} \le P_T. \qquad (30-f)$$

where $\boldsymbol{\beta_k}(\mathbf{q},\boldsymbol{v}) \triangleq \gamma(\boldsymbol{v}^H\overline{\boldsymbol{\Psi}}_{\boldsymbol{k}}(\mathbf{q})\,\boldsymbol{v}+\sigma^2)$, $\boldsymbol{\alpha}(\mathbf{q},\boldsymbol{v}) \triangleq \frac{\boldsymbol{v}^H\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}}{q_s}$, $\kappa(\mathbf{q},\mu) \triangleq \frac{\tau_{RJ_1}\left|h_{l^*-J_1}\right|^2}{q_{J_1}}\mu + \frac{\tau_{RS}|f_{Rl^*}|^2}{q_s}\mu + \sigma^2\mu$, and $\xi(q_s) \triangleq \frac{|\mathrm{f}_{Rl^*}|^2}{q_s}$. In the following, we first investigate the convexity of the objective function (30) and the constraints (30-a)-(30-f) through some observations.

O1) The arguments $\frac{1}{q_{J_1}}$ and $\frac{1}{q_s}$ are strictly convex functions with respect to q_{J_1} and q_s, respectively [35, Sec. 3.1]. As a consequence, $\mathbf{1}_2^T\mathbf{q}$ which is the summation of convex functions is also a strictly convex function over $\mathbf{q}$ [35, Sec. 3.2]. Similarly, we can ascertain the convexity of the terms $\kappa(\mathbf{q},\mu)$ and $\xi(q_s)$ with respect to q_s and q_{J_1}.

O2) The argument $\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k(\mathbf{q})\,\boldsymbol{v}$ that appeared in the objective function, of (30) includes the summation of the quadratic form function $\sigma^2\boldsymbol{v}^H\boldsymbol{v}$ and of the quadratic-over-linear functions $(1+\tau_{RS})\,\boldsymbol{v}^H\mathbf{H}^H\mathbf{F}_{R_{-1}}\mathbf{F}_{R_{-1}}^H\mathbf{H}\boldsymbol{v}/q_s$, $\tau_{RJ_1}\mathbf{H}^H\mathbf{H}_{R_{-1}}$ $\mathbf{H}_{R_{-1}}^H\mathbf{H}/q_{J_1}$. As it is widely acknowledged, the well-known quadratic form $\boldsymbol{z}^H\boldsymbol{A}\boldsymbol{z}$ is convex over the variable $\boldsymbol{z}$ if the matrix $\boldsymbol{A}$ is a Hermitian positive semidefinite [35, Sec. 4.2]. Moreover, for $g > 0$ the quadratic-over-linear function $\frac{\boldsymbol{z}^H\boldsymbol{A}\boldsymbol{z}}{g}$, which is also known as the perspective function of $\boldsymbol{z}^H\boldsymbol{A}\boldsymbol{z}$ is jointly convex over the variables $(\mathbf{z},g)$ [35, Sec. 3.2.6]. Hence, $\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k(\mathbf{q})\,\boldsymbol{v}$ where $\overline{\boldsymbol{\Upsilon}}_k(\mathbf{q}) \succcurlyeq 0$, is a joint convex function in $(\mathbf{q},\boldsymbol{v})$ [35, Sec. 3.4]. Similarly, the joint convexity of the terms $\boldsymbol{\beta}_k(\mathbf{q},\boldsymbol{v})$, $\boldsymbol{\alpha}(\mathbf{q},\boldsymbol{v})$, and $\boldsymbol{v}^H\overline{\boldsymbol{\Upsilon}}_k^{l,l}(\mathbf{q}\ )\,\boldsymbol{v}$ over $(\mathbf{q},\boldsymbol{v})$ can be inferred, as well.

As a direct application of O1 together with O2, it can be inferred that the objective function $\mathcal{D}_k(\mathbf{q},\boldsymbol{v})$ and the constraints (30-c)-(30-f) are convex, whereas the constraints (30-a) and (30-b), including the difference of two convex functions are still non-convex constraints. To handle this non-convexity, we resort to the classic CCCP technique which is an algorithm broadly used for solving the DC programs [33], [34]. The main idea behind the CCCP is to iteratively approximate the non-convex feasible set in (30-a) and (30-b) around the current point by a convex subset. The resultant convex approximation can be efficiently solved via the standard primal-dual interior point methods [35, Sec. 11.7]. Notably, although our proposed method mainly relies on the CCCP technique, it is different from the conventional CCCP of [33] wherein the CCCP is initialized to a random (may be infeasible) point and may fail at the first iteration owing to its infeasibility. Hence, a novel initialization is introduced in this paper in which a feasible point of the DC program is acquired from the proposed feasible initial points search algorithm (FIPSA).

Algorithm 1 Joint OPA-CANB design algorithm:

```
**Input:** Set the threshold value for accuracy: $\delta_x$ and the maximum number of iterations: $N_{max}$
**Initialization:** Initialize $\mathbf{t}^{(0)}$. Set the iteration number $n = 0$
**Calculating the optimal:** $P_s^\circ$, $P_{J_1}^\circ$,$\boldsymbol{v}^\circ$
**While** $\left\{\left|\mathcal{D}_k\left(\mathbf{t}^{(n+1)},\mathbf{t}\right) - \mathcal{D}_k(\mathbf{t}^{(n)},\mathbf{t})\right| \le \delta_x \text{ or } n \le N_{max}\ \right\}$
 **do (1) to (4):**
 **(1).**Calculate $\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)$ and $\widehat{\mho}_k(\mathbf{q}^{(n)},\mathbf{q})$
 **(2).** Solve (31), then assign the solution to $\mathbf{t}^{(n+1)}$.
 **(3).** Update the slack variable $\mu$ based on $\mathbf{t}^{(n+1)}$.
 **(4).** $n = n + 1$
 **End While,**
 **Calculating the optimal:** $P_{J_2}^\circ$, $\boldsymbol{\sigma}^\circ$
 Solve (34) to achieve $\boldsymbol{\sigma}^\circ$ and $P_{J_2}^\circ$
**Output:** $\mathbf{t}^\circ$, $P_{J_2}^\circ$ , $\boldsymbol{\sigma}^\circ$
```

2) The Proposed Iterative Optimization algorithm to Solve $\mathbf{P_1}$*:* In this section, the DC program (30) is efficiently solved via our proposed CCCP-based algorithm. As mentioned earlier, the CCCP-based algorithm tries to approximate the non-convex feasible set by a convex subset in each iteration. In the proposed method here, the approximation is accomplished through the first order Taylor expansion of the non-convexity factor around the current point. For the sake of notational simplicity, the shortened variable of $\mathbf{t} \triangleq \left[\mathbf{q}^T, \boldsymbol{v}^T\right]^T$ is utilized hereafter. Accordingly, as seen from $\mathcal{T}_k(\mathbf{t})$, the non-convexity has resulted from the convex part $\boldsymbol{\alpha}(\mathbf{t})$. Therefore, by exploiting the Taylor expansion, an appropriate affine approximation set of real-valued function $\boldsymbol{\alpha}(\mathbf{t})$ at the nth iteration and around the current complex-valued vector $\mathbf{t}^{(n)}$, denoted by $\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)$, is achieved as follows (see, e.g., [36, Theorems 3 and 4])

$$\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right) = \boldsymbol{\alpha}\left(\mathbf{t}^{(n)}\right) + 2\mathfrak{Re}\left\{\boldsymbol{\nabla\alpha}\left(\mathbf{t}^{(n)}\right)^H\left(\mathbf{t}-\mathbf{t}^{(n)}\right)\right\}, \qquad (31)$$

where $\boldsymbol{\nabla\alpha}\left(\mathbf{t}^{(n)}\right)^H$ denotes the conjugate derivation operator of the function $\boldsymbol{\alpha}\left(\mathbf{t}^{(n)}\right)$ with respect to the point $\mathbf{t}^{(n)} \triangleq \left[\mathbf{q}^{(\boldsymbol{n})T}, \boldsymbol{v}^{(\boldsymbol{n})T}\right]^T$ which can be written as $\boldsymbol{\nabla\alpha}\left(\mathbf{t}^{(n)}\right)^H = \left[\frac{\boldsymbol{v}^{(\boldsymbol{n})H}\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}^{(\boldsymbol{n})}}{-2\left(q_s^{(n)}\right)^{\mathbf{2}}}, \left(\frac{\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}^{(\boldsymbol{n})}}{q_s^{(n)}}\right)^T\right]^T$.By substituting $\boldsymbol{\nabla\alpha}\left(\mathbf{t}^{(n)}\right)^H$into (31) and following some further manipulation, the affine approximation expression $\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)$ is reformulated as (32) on top of next page. We also attain the first order Taylor expansion of $\xi\left(q_s\right)$ (i.e., $\widehat{\xi}\left(q_s\right)$), leading to a convex form of $\mho_k(\mathbf{q})$. Substituting $\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)$ and $\widehat{\xi}\left(q_s\right)$ into (30-a) and (30-b), yields the following proposed CCCP-based iterative algorithm in which a convex optimization problem is solved at the nth iteration, rather than using the previous original non-convex form (30)

$$\mathbf{P}_3: \ \min_{\mathbf{t}} \mathcal{D}_k(\mathbf{t}), \tag{33}$$

s.t.

$$\widehat{\mathcal{T}}_k(\mathbf{t}^{(n)},\mathbf{t}) \triangleq \boldsymbol{\beta}_k\left(\mathbf{t}\right) - \widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right) \leq 0, \tag{33-a}$$

$$\widehat{\mho}_k(\mathbf{q}^{(n)},\mathbf{q}) \triangleq \kappa\left(\mathbf{q},\mu\right) - \widehat{\xi}\left(q_s^{(n)},q_s\right) \leq 0, \tag{33-b}$$

$$\mathcal{D}_k^{l,l}\left(\mathbf{t}\right) - Q_l \leq 0 \ , \forall l \in \mathcal{L}, \tag{33-c}$$

$$\tfrac{1}{q_{J_1}} + \tfrac{1}{q_s} + \mathcal{D}_k\left(\mathbf{t}\right) - Q_{tot} \leq 0, \tag{33-d}$$

$$\tfrac{1}{q_{J_1}} - \overline{P}_{J_1} \leq 0, \tag{33-e}$$

$$\tfrac{1}{q_s} - P_T \leq 0. \tag{33-f}$$

where we have, $\widehat{\xi}\left(q_s^{(n)},q_s\right) = |\mathrm{f}_{Rl^*}|^2.\left(\frac{1}{q_s^{(n)}} - \frac{\left(q_s - q_s^{(n)}\right)}{q_s^{(n)2}}\right)$. This procedure will be continued until some stopping criterion is satisfied or the number of predefined iterations is reached. We note that, due to the convexity of the functions $\boldsymbol{\alpha}\left(\mathbf{t}\right)$, its first-order Taylor approximation is reduced at each iteration, i.e., we have $\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right) \leq \boldsymbol{\alpha}\left(\mathbf{t}\right)$, which is responsible for increasing the constraint (33-a) at each iteration. Therefore, the convex function $\widehat{\mathcal{T}}_k\left(\mathbf{t}^{(n)},\mathbf{t}\right) \triangleq \boldsymbol{\beta}_k\left(\mathbf{t}\right) - \widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)$ in (33-a) can be taken into account as a strengthening form of its non-convex form $\mathcal{T}_k(\mathbf{t}) \triangleq \boldsymbol{\beta}_k\left(\mathbf{t}\right) - \boldsymbol{\alpha}\left(\mathbf{t}\right)$ in (30-a). Given this perspective, the feasible set belonging to $\widehat{\mathcal{T}}_k\left(\mathbf{t}^{(n)},\mathbf{t}\right)$ always lies within the true feasible set defined in $\mathcal{T}_k(\mathbf{t})$. A similar discussion can be conceived for $\widehat{\xi}\left(q_s^{(n)},q_s\right)$ and $\widehat{\mho}_k(\mathbf{q}^{(n)},\mathbf{q})$. Therefore, if the initial feasible point $\mathbf{t}^{(0)}$ exists for the general non-convex form (30), all the points produced throughout the iterations , $\left\{\mathbf{t}^{(n)}\right\}$ $n = 1, 2, , \ldots,$ by iteratively solving the convex form (33), always lies within the true feasible set of the original non-convex form (33).

In summary, a low-complexity solution was provided above in which a simple convex optimization problem was solved in contrast to the hard-to-solve non-convex problem (30). By assuming that an initial feasible point $\mathbf{t}^{(0)}$ is available for the general problem (30), the proposed solution converges to a local minimum after a few iterations (See Appendix for proof).

Algorithm 2 The proposed CCCP-based FIPSA:

```
Input: Set the threshold value for accuracy: $\delta_I$and the maximum number of iterations: $M_{max}$
Initialization: Initialize the algorithm with arbitrary random point $\mathbf{t}^{(0)}$. Set the iteration number $n = 0$
While $\left\{\boldsymbol{z}^{(n)} \leq \delta_I \text{ or } n \leq M_{max}\ \right\}$ do (1) to (3):
  (1). Calculate $\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)$ and $\widehat{\mho}(\mathbf{q}^{(n)},\mathbf{q})$.
  (2). Solve the problem (37),
  (3). $n = n + 1$
  End While,
Output: $\mathbf{t}^{\circ}$ ,$z^{\circ}$
```

B. Second Sub-Problem

Given the resultant optimal values $\boldsymbol{v}^{\circ}$, P_s°, as well as $P_{J_1}^{\circ}$, the power consumption at each relay node formulated as $P_{I,l}^{\circ} \triangleq \boldsymbol{v}^{\circ H}\overline{\boldsymbol{\Upsilon}}_k^{l,l}\left(\overline{\mathbf{P}}^{\circ}\right)\boldsymbol{v}^{\circ}$, $\forall l \in \mathcal{L}$, and the total power $P_I^{\circ} \triangleq \boldsymbol{v}^{\circ H}\overline{\boldsymbol{\Upsilon}}_k\left(\overline{\mathbf{P}}^{\circ}\right)\boldsymbol{v}^{\circ}$ allocated for retransmitting the desired information by the relay nodes, can be computed. The remaining power $Q_l^{'} \triangleq Q_l - P_{I,l}^{\circ}$ is dedicated to each relay node for transmitting AN in order to enhance the security of the system. We also note that the new power budget $Q_{tot}^{'} \triangleq Q_{tot} - P_s^{\circ} - P_{J_1}^{\circ} - P_I^{\circ}$ is assigned for AN transmission during phase II, i.e., $P_{AN}^{(2)} \triangleq P_{AN} + P_{J_2}$. Subject to these new power constraints, in the second sub-problem solved in this section we aim for maximizing the total power allocated to $P_{AN}^{(2)}$, for eliminating the information leakage as much as possible. It should be noted that, the AN $\mathbf{n}_{a,l}$ emitted by lth relay node can be written as $\mathbf{n}_{a,l} \triangleq \mathbf{U}^{(l)}\boldsymbol{z} = \sum_{k=1}^{N-2} u_{l,k}z_k$, where $\mathbf{U}^{(l)}$ denotes the lth row of $\mathbf{U}$. Consequently, the power assigned to AN transmission at the lth relay node can be obtained as $P_{\mathrm{n}_{a,l}} \triangleq \overline{\mathbf{U}}^{(l)}\boldsymbol{\sigma} = \sum_{k=1}^{N-2} |u_{l,k}|^2\sigma_{z,k}^2$ where $\overline{\mathbf{U}} \in \mathbb{C}^{(N-1)\times(N-2)}$ is defined as a matrix whose elements are represented in the form of $\left[\overline{\mathbf{U}}\right]_{l,k} \triangleq |u_{l,k}|^2$. Now, defining $\mathbf{Q}_m \triangleq \left[Q_1^{'},\ Q_2^{'}, \ldots, Q_{N-1}^{'}\right]^T$, based on the original max-min optimization problem (27), one can obtain the second sub-problem as follows:

$$\mathbf{P}_4: \max_{\sigma_{z,k}^2, P_{J_2}} \ \mathcal{C}(\boldsymbol{\sigma}, P_{J_2}) \triangleq \mathbf{1}_{N-2}^T\boldsymbol{\sigma} + P_{J_2}, \tag{34}$$

s.t.

$$\overline{\mathbf{U}}\boldsymbol{\sigma} \leq \mathbf{Q}_m, \tag{34-a}$$

$$\mathcal{C}(\boldsymbol{\sigma}, P_{J_2}) \leq Q_{tot}^{'}, \tag{34-b}$$

$$0 < P_{J_2} \leq \overline{P}_{J_2}. \tag{34-c}$$

The constraints (34-a)-(34-b) can be unified and rewritten in the form of a single linear constraint as $\overline{\mathbf{U}}_{tot}\boldsymbol{\psi}_{\sigma,p} = \mathbf{b}$ where $\overline{\mathbf{U}}_{tot}$, $\boldsymbol{\psi}_{\sigma,p}$ and $\mathbf{b}$ are obtained as

$$\overline{\mathbf{U}}_{tot} \triangleq \begin{bmatrix} \overline{\mathrm{U}}_{11} & \overline{\mathrm{U}} & \ldots & \overline{\mathrm{U}}_{1,N-2} & 0 \\ \overline{\mathrm{U}}_{21} & \overline{\mathrm{U}}_{22} & \ldots & \overline{\mathrm{U}}_{2,N-2} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \overline{\mathrm{U}}_{N-1,1} & \overline{\mathrm{U}}_{N-1,2} & \ldots & \overline{\mathrm{U}}_{N-1,N-2} & 0 \\ 1 & 1 & \ldots & 1 & 1 \end{bmatrix},$$

$$\mathbf{b} \triangleq \left[\mathbf{Q}_m^T, Q_{tot}^{'}\right]^T, \boldsymbol{\psi}_{\sigma,p} \triangleq \left[\boldsymbol{\sigma}^T, P_{J_2}\right]^T, \tag{35}$$

Therefore, we now have a linear programming (LP) problem, which can be easily solved to obtain the optimal $\boldsymbol{\sigma}^{\circ}$ and $P_{J_2}^{\circ}$ as follows :

$$\mathbf{P}_5: \max_{\sigma_{z,k}^2, P_{J_2}} \ \mathcal{C}(\boldsymbol{\sigma}, P_{J_2}), \tag{36}$$

s.t.

$$\widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)},\mathbf{t}\right)=\mathfrak{Re}\left\{\frac{\boldsymbol{v}^{(\boldsymbol{n})^H}\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}^{(\boldsymbol{n})}}{q_s^{(n)}}\right\}-\frac{\boldsymbol{v}^{(\boldsymbol{n})^H}\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}^{(\boldsymbol{n})}}{q_s^{(n)}}-\frac{\boldsymbol{v}^{(\boldsymbol{n})^H}\overline{\boldsymbol{\Phi}}_{Gf}\boldsymbol{v}^{(\boldsymbol{n})}}{\left(q_s^{(n)}\right)^{\mathbf{2}}}\left(q_s-q_s^{(n)}\right). \tag{32}$$

$$\overline{\mathbf{U}}_{tot}\boldsymbol{\psi}_{\sigma,p}\preccurlyeq\mathbf{b}, \qquad (36-a)$$

$$[\boldsymbol{\sigma}]_{\boldsymbol{n}}\geq 0, \qquad (36-b)$$

$$0<P_{J_2}\leq\overline{P}_{J_2}. \qquad (36-c)$$

V. Implementation

The proposed low-complexity solution of the original problem (27) and the determination of the optimal points P_s°, $P_{J_1}^\circ$, $\boldsymbol{v}^\circ$, $P_{J_2}^\circ$, and $\boldsymbol{\sigma}^\circ$ is summarized in Algorithm 1. By assuming that an initial feasible point of the DC program (33), i.e., $\mathbf{t}^{(0)}$, is available, we first compute the optimal points $P_s^\circ=\frac{1}{q_s^\circ}$, $P_{J_1}^\circ=\frac{1}{q_{J_1}^\circ}$, and $\boldsymbol{v}^\circ$ in an iterative procedure by using the affine approximation of the DC program. This procedure will then be continued until the difference of the objective function $\mathcal{D}_k(\mathbf{t})$ in successive iterations becomes smaller than the predefined threshold value δ_x, i.e., until we have $\left|\mathcal{D}_k\left(\mathbf{t}^{(n+1)},\mathbf{t}\right)-\mathcal{D}_k(\mathbf{t}^{(n)},\mathbf{t})\right|\leq\delta_x$, or the number of maximum affordable iteration is reached. In the next step, given these optimal points obtained, we can readily calculate $\boldsymbol{\sigma}^\circ$ and $P_{J_2}^\circ$ via the LP problem of (36).

VI. The Proposed CCCP-Based FIPSA

In contrast to the conventional CCCP, which starts with an arbitrary random point [33], we have assumed in Algorithm I that it is initialized with a *feasible* point of the DC program. Again, for the conventional CCCP, the algorithm may fail at the first iteration due to the infeasibility, while upon invoking the proposed novel initialization method here the well-suited feasible initial points (FIP) are pre-calculated. Hence, we can not only guarantee for the algorithm to avoid this failure, but also all the solutions iteratively produced by Algorithm 1 belong to the original feasible set of the DC program. However, it has been demonstrated in [37] that, by computing the feasible point for the DC program (30), which is also a non-convex problem is generally NP-hard. Therefore, inspired by [35, Sec. 11.4] and [38] we develop an efficient search algorithm to find an FIP of the DC program (30). In this regard, we should solve another minimization problem which relies on minimizing the real-valued slack parameter $z\geq 0$ that can be regarded as a measure of constraint violations or in other words a measure of how far the relevant constraints in (33-a) and (33-b) are from being satisfied. Hence it acts as *an infeasibility indicator*. The proposed FIPSA can be formulated as the following convex program, which exploits the same CCCP-based affine approximations $\widehat{\mathcal{T}}_k(\mathbf{t}^{(n)},\mathbf{t})$ and $\widehat{\mho}_k(\mathbf{q}^{(n)},\mathbf{q})$.

$$\mathbf{P}_6:\min_{z,\mathbf{t}} z, \tag{37}$$

s.t.

$$\widehat{\mathcal{T}}_k(\mathbf{t}^{(n)},\mathbf{t})\leq z, \qquad (37-a)$$

$$\widehat{\mho}_k(\mathbf{q}^{(n)},\mathbf{q})\leq z, \qquad (37-b)$$

$$\mathcal{D}_k^{l,l}(\mathbf{t})-Q_l\leq z\ ,\ \forall l\in\mathcal{L}, \qquad (37-c)$$

$$\tfrac{1}{q_{J_1}}+\tfrac{1}{q_s}+\mathcal{D}_k\left(\mathbf{t}\right)-Q_{tot}\leq z. \qquad (37-d)$$

The objective value z at the current iteration, i.e., $z^{(n+1)}$, is equal to the minimum value among the various thresholds provided by the different constraints as

$$z^{(n+1)}=\min\Bigg\{\widehat{\mathcal{T}}_k\left(\mathbf{t}^{(n)},\mathbf{t}\right),\widehat{\mho}_k\left(\mathbf{q}^{(n)},\mathbf{q}\right),$$
$$\left\{\mathcal{D}_k^{l,l}(\mathbf{t})-Q_l,\ \ \forall l\in\mathcal{L}\right\},\frac{1}{q_{J_1}}+\frac{1}{q_s}+\mathcal{D}_k\left(\mathbf{t}\right)-Q_{tot}\Bigg\}, \tag{38}$$

The algorithm continues unless $z^{(n+1)}$ in the successive iterations becomes smaller than the predefined threshold value or the maximum number of allowable iterations is reached. Additionally, the algorithm is terminated in the case when $z^{(n+1)}$ becomes zero. As the final stage, the point $\mathbf{t}^{(n+1)}$ has to be checked if it is feasible or not, by substituting it back into (30). In what follows, the proposed CCCP-based FIPSA is presented as Algorithm 2. It should be noticed that, although the outcome of Algorithm 2 always lies within the original feasible set of the original DC program (30), only a subset of the original feasible sets are obtained through Algorithm 2. Therefore, it cannot be inferred that the original problem (30) is infeasible, if the proposed Algorithm 2 fails to provide a feasible point.

It should be mentioned that, the overall algorithm is accomplished in two consecutive phases, where the proposed FIPSA Algorithm 2 yields a proper FIP at the first stage and then, given this FIP, the optimal points $\mathbf{t}^\circ$, $P_{J_2}^\circ$, and $\boldsymbol{\sigma}^\circ$ are acquired through Algorithm 1.

VII. Numerical results and discussions

In this part, several numerical examples are presented to highlight the merits of the proposed joint CB, jamming and power allocation in the presence of untrusted relays and a passive Eve. Furthermore, for simplicity and without loss of generality, the source, the destination and the relays are assumed to be placed at the positions $(-1,0),(1,0)$ and $(0,0)$, respectively. Moreover, our simulation settings are listed as follows, unless otherwise stated: the threshold values for the stopping criteria of Algorithm 1 and of FIPSA are respectively $\delta_x=\delta_I=10^{-3}$, the impairments at each node are $k_i^t=k_i^r=0.08$, the number of antennas at Eve is$N_E=2$, the Gaussian noise power $\sigma^2=10^{-3}$, $Q_l=\frac{2Q_{tot}}{L}$ and $P_T=1.5Q_{tot}$. Moreover, in the numerical results, the hybrid jamming (HJ) policy, which was discussed in Section III. A,

TABLE I
PARAMETERS USED IN DIFFERENT COMPARATIVE SCHEMES THROUGHOUT THE EXPERIMENTS

Scheme Number	**Algorithm Used To Obtain Optimal values**	**Number of Relays**	**Total Power Budget (Q_{tot})**	**Minimum Required QoS (γ_{min})**	**Type of Relay Node**	**Jamming Strategy at Phase I**	**Jamming Power budget at Phase I ($\overline{P}_{J_1}$)**	**Impairment Level at Each Node k_i^t, k_i^r**
Scheme 1	Alg. 2	$4, 12$	25 dBm	4dB	Untrusted	-----------	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 2	Alg. 1 after Alg.2	$8, 16$	-----------	$4, 12$ dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 3	Alg. 1 after Alg.2	$8, 16$	-----------	$4, 12$ dB	Trusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 4	Alg. 1 after Alg.2	$8, 12$	-----------	4dB	Untrusted	DACJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 5	Alg. 1 after Alg.2	$8, 12$	-----------	4dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 6	Alg. 1 after Alg.2	8	25 dBm	$4, 12$ dB	Untrusted	DACJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 7	Alg. 1 after Alg.2	8	25 dBm	$4, 12$ dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 8	Alg. 1 after Alg.2	10	25 dBm	12 dB	Untrusted	DACJ	$P_{J_1}^{opt}$	0.08
Scheme 9	Alg. 1 after Alg.2	10	25 dBm	12 dB	Untrusted	HJ	$P_{J_1}^{opt}$	0.08
Scheme 10	Alg. 1 after Alg.2	10	25 dBm	12 dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	0.08
Scheme 11	Alg. 1 after Alg.2	8	50 dB	12 dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	$0, 0.08, 0.16$
Scheme 12	Alg. 1 after Alg.2	$8, 12$	-----------	12 dB	Untrusted	HJ	$Q_l \in [0, 40]$	0, 0.08
Scheme 13	Alg. 1 after Alg.2	$4, 16$	35 dBm	12 dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	$K_i^t + K_i^r = 0.2, i \in \{S, D\}, R$
Scheme 14	Alg. 1 after Alg.2	8	25 dBm	4 dB	Untrusted	HJ	$Q_l = \frac{2Q_{tot}}{L}$	0, 0.08
Scheme 15	Alg. 1 after Alg.2	8	25 dBm	4 dB	Untrusted	DACJ	$Q_l = \frac{2Q_{tot}}{L}$	0, 0.08

is adopted for jammer selection. The numerical results are presented to quantify the secrecy performance of the proposed method, and all of the numerical results were averaged over 2000 independent channel realizations.

In the following, in order to make a final conclusion easier and more tangible, we collect various comparative schemes, used in the experiments, in Table I. Fig. 4 depicts the average convergence of the FIPSA Algorithm using the OF value of (37) versus the number of iterations for two different number of untrusted relays, i.e., Scheme 1. The relevant simulation parameters have been depicted in the first row of Table I. As observed, the average convergence of the FIPSA Algorithm is fast, since it is converged during three iterations. Furthermore, we can see in Fig. 4 that as the number of relays grows, the algorithm's convergence rate increases.

Fig. 5 shows the average secrecy rate achieved by the proposed Algorithm versus the total power budget. The secrecy rate is computed by substituting (20), (21)as well as (26) into (18). In this figure, we aim for comparing the secrecy rate of the proposed untrusted relaying (i.e., Scheme 2) with the trusted relaying scenario (i.e., Scheme 3) for different number of relays and different required QoS expressed in $bits/s/Hz$. The associated simulation parameters of Scheme 2 and Scheme 3 have been respectively shown in the second and third rows of Table I. This figure states that the trusted relaying scenario outperforms the untrusted relaying for small and medium total power budgets. However, as the total power budget becomes high, the secrecy rate of both the trusted and untrusted relaying becomes similar. The reason for this is that at high transmit powers, there is sufficient power budget to support both the security and reliability requirements. We can also observe that given a specific total power budget, the secrecy rate increases as the number of relays grows. This is because by increasing the number of relays, the network's degree of freedom is increased, hence enhancing the achievable secrecy rate. We note that since in this paper our

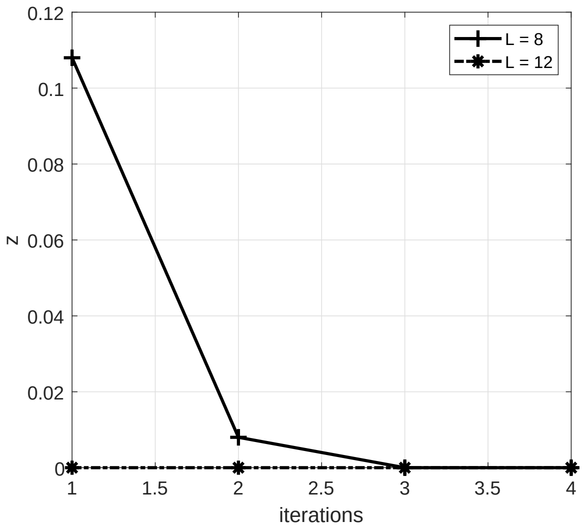


Fig. 4. Evaluating of convergence behavior of the FIPSA through depicting the OF value in (39-a) versus the number of iterations for parameters of Scheme 1 shown in Table I.

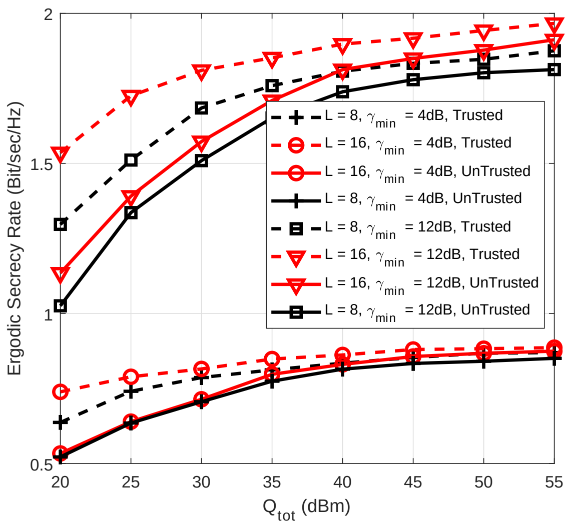


Fig. 5. Average secrecy rate achieved by the proposed algorithm versus the total power budget for the parameters used in Scheme 2 and Scheme 3 mentioned in Table I.

goal is to guarantee the minimum required QoS, γ_{min}, while the remaining power is dedicated to inject AN, therefore, the maximum achievable secrecy rate will be $\frac{1}{2}\log_2(1+\gamma_{min})$.

To reveal the impact of different number of untrusted relays (i.e., Schemes 4 and 5) and various desired QoS values γ_{min} (i.e., Schemes 6 and 7), for two different jamming strategy, we have provided Figs. 6 and 7. The related parameters used in this simulation, can be found in Table I, as well. In Fig. 6, one can observe the impact of the number of untrusted relays on the achievable secrecy rate, when developing the proposed algorithm. As it can be seen, upon increasing the number of relays, the secrecy rate of the DACJ policy (i.e., Scheme 4) is enhanced by about $0.1\,bits/s/Hz$, while no significant secrecy rate enhancement is obtained for the HJ policy (i.e., Scheme 5). Actually, if the DACJ policy is applied, the intended receiver can decode the source information by cancelling the self-interference signal at the second phase. Therefore, the relays do not require to perform BF for eliminating the jamming AN $z^{(1)}$ at the destination and thus they take advantages of provided degrees of freedom for further increasing the secrecy rate. While, in the case of utilizing HJ, which is the combination of both FACJ and DACJ, it is more likely for one of the relay to be chosen as jammer. In this case, the NSB design is inevitably necessary to cancel the jamming signal at the destination, contributing to reducing the degrees of freedom at relays. On the other hand, owing to inherent impairment existing in the system, this NSB cannot thoroughly prevent the interference leaked towards the intended receiver. As a result, increasing the relay nodes is accompanied with boosting the interference leakage due to unwanted noises at the destination. In contrast to Fig. 6, in Fig. 7 we study the impact of various QoS requirements on the average secrecy rate. As observed, the HJ policy (Scheme 6) outperforms the DACJ policy (Scheme 7), especially for large Q_{tot}.

Fig. 8 depicts the average secrecy rate of different jammer selection scenarios versus the number of iterations (i.e., Schemes 8, 9, and 10). Although the HJ policy (Schemes 9 and 10) provides better secrecy rate than the DACJ (Scheme 8), the computational complexity of selecting the best relay and the processing overhead required for the HJ increases as the number of relays grows. By contrast, the DACJ policy benefits from a low-implementational complexity and it is suitable for networks having limited processing resources such as ad-hoc and sensor networks. From this figure, we also find that even if the HJ utilizes the non-optimal power of $P_{J1} = P_{J1}^{max} = Q_l$ (Scheme 10), its secrecy rate remains better than that of the DACJ policy relying on the optimal power P_{J1}^{opt} (Scheme 8), which is obtained through an exhaustive search. As previously mentioned in remark 2, setting P_{J_1} at its upper bound in jammer selection stage, i.e., $P_{J1} = Q_l$, is an appropriate choice for finding the suboptimum jammer. As observed in Fig. 8, although using P_{J1}^{opt} results in a better average secrecy rate rather than selecting $P_{J1} = Q_l$, the resultant difference can be negligible in contrast to the computational overhead imposed to find P_{J1}^{opt}.

We have provided Figs. 9 and 10 to highlight the impact of the jamming power at Phase I both on the average secrecy rate and on the power required for the information signal $(P_I + P_s)$ and jamming at Phase II $(P_{AN} + P_{J2})$. The simulation parameters in associated with this experiment can be found in the corresponding row of Scheme 11 in Table I. These figures show that most of the total power should be allocated to the jammer at Phase I to enhance the PLS. We note that the only protection mechanism at Phase I is the cooperative jamming relying on the power of P_{J1}. As the budget dedicated for this jamming power increases, the communication becomes more robust against passive eavesdropping attack. Hence the secrecy rate is also increased. At the second phase, the information leakage is negligible owing to the presence of HIs and as a consequence of the AN imposed by the relays. Therefore, most of the information is leaked during the first phase of transmission. Furthermore, based on what was discussed about

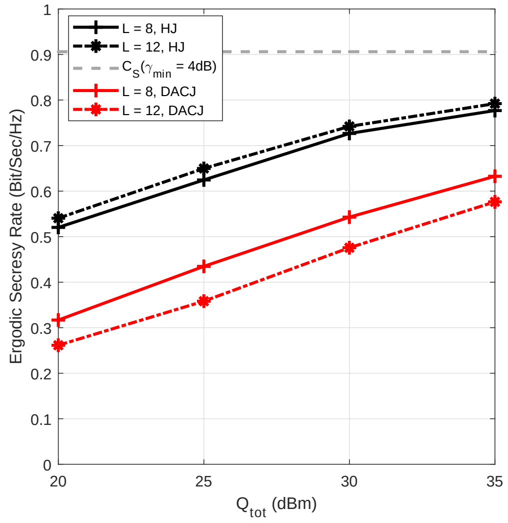


Fig. 6. Average secrecy rate achieved by the proposed algorithm versus the total power budget for Scheme 4 and Scheme 5 mentioned in Table I.

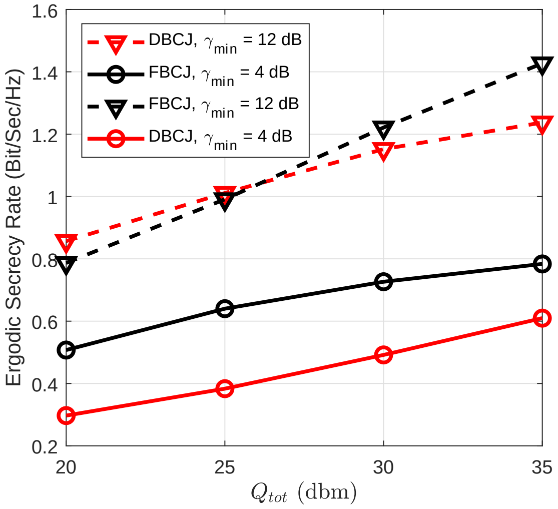


Fig. 7. Average secrecy rate achieved by the proposed algorithm versus the total power budget for Scheme 6 and Scheme 7 mentioned in Table I.

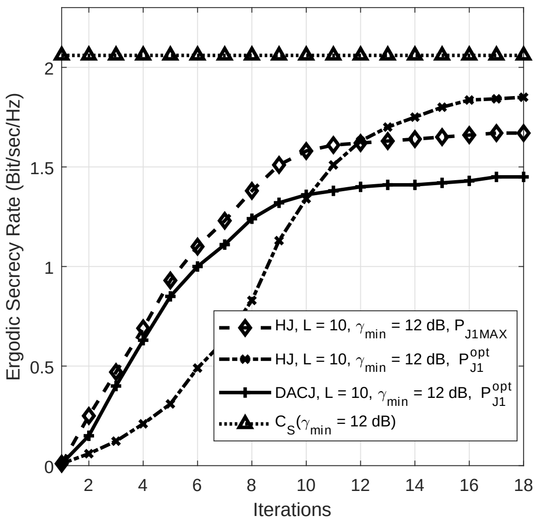


Fig. 8. Average secrecy rate achieved by the proposed algorithm versus the number of iterations for Schemes (8-10), mentioned in Table I.

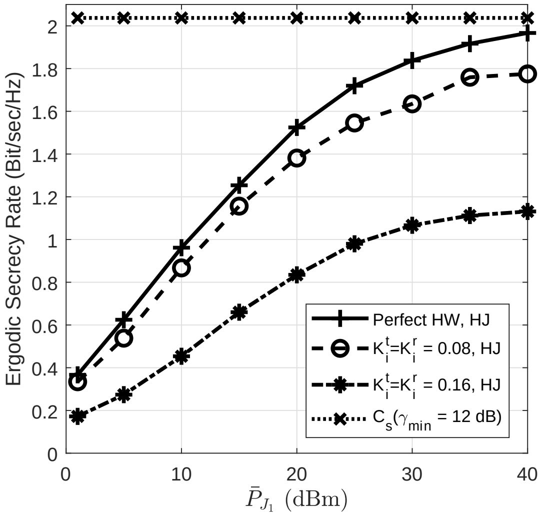


Fig. 9. Average secrecy rate versus the jamming power budget ($\overline{P}_{J_1}$) for Scheme 11, mentioned in Table I.

Fig. 8, we also note that since the secrecy rate is an increasing function of P_{J1} with $P_{J1} \leq Q_l$, the assumption of $P_{J1} = Q_l$ constitutes the optimum. Observe from figures 8 and 9, it can be inferred that by increasing the level of HIs, the power $(P_I + P_s)$ required for information transmission is increased. Furthermore, the

average secrecy rate is confined to a ceiling. An interesting observation from Fig. 10 is that as the jamming power budget $\overline{P}_{J1}$ is increased, the AN power $(P_{J2} + P_{AN})$ injected at the second phase remains approximately constant while the power $(P_I + P_s)$ assigned to the information signal grows. This is because of the fact that, given the specific value of γ_{min}, the network is capable of maintaining the minimum reliability requirement at the legitimate terminal D by a small amount of $P_I + P_s$. As such, the remaining power, which constitutes the significant portion of the total power budget Q_{tot}, will be assigned to the AN power $P_{J2} + P_{AN}$.

Observe in Fig. 11, the power required for information transmission is reduced upon increasing the number of untrusted relays. The relevant parameters used in this simulation, can be found in corresponding row of Scheme 12 of Table I. This is because of the fact that by increasing the number of untrusted relays, the information leakage is increased. Consequently, to enhance the PLS, most of the total power for achieving a fixed target $\gamma_{min} = 12$ dB have to be allocated for AN, and thus the power assigned for information transmission, i.e., $(P_I + P_s)$ is decreased. Moreover, as it is earlier observed in Fig. 10, we can also see from Fig. 11 that increasing the level of HIs, is responsible for boosting the power $(P_I + P_s)$.

We plot Fig. 12 to present some engineering insights for

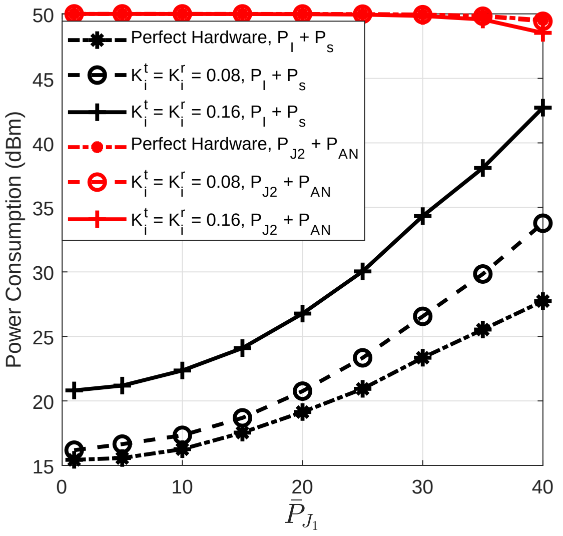


Fig. 10. Average power consumption versus the jamming power budget ($\bar{P}_{J_1}$) for Scheme 11, mentioned in Table I.

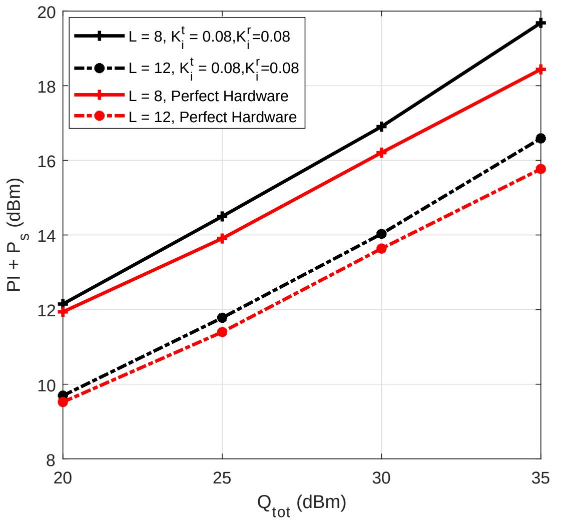


Fig. 11. Average information power consumption versus the total power budget with the parameters used in Scheme 12 of Table I.

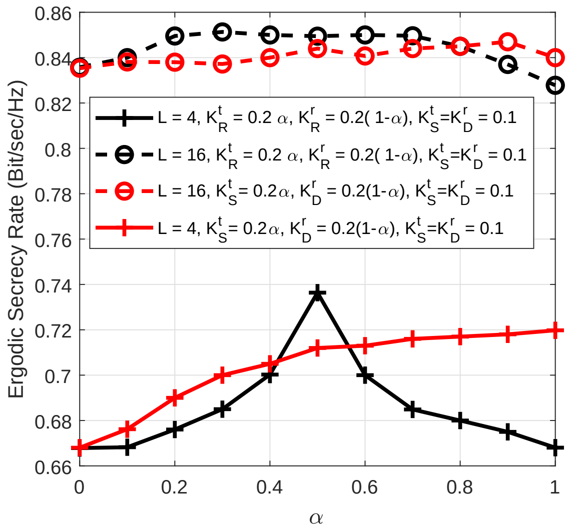


Fig. 12. Average secrecy rate versus different values of impairments at source, relay and destination, under the assumption of $K_i^t + K_i^r = 0.2$. The simulation parameters are presented in Scheme 13 of Table I.

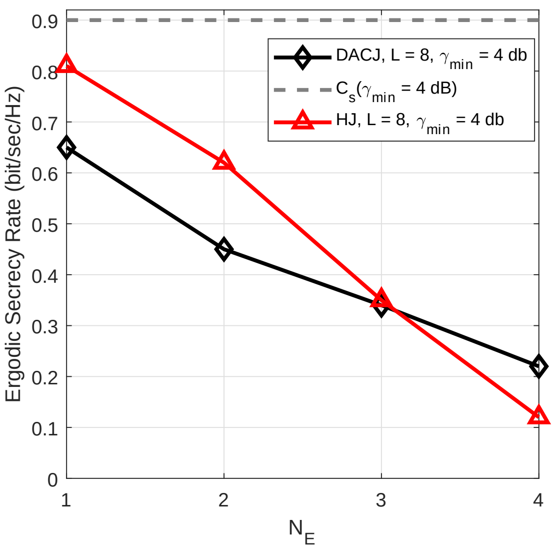


Fig. 13. Average secrecy rate achieved by the proposed algorithm versus the Number of Eve's antenna for Scheme 14 and 15 mentioned in Table I.

designing practical networks. To produce Fig. 12 we have assumed that the HI imposed on the reception and transmission sections of each node equals to 0.1 such that $K_i^t + K_i^r = 0.2$ for $i \in \{S, D\}$, or $K_R^t + K_R^r = 0.2$. The question is that how the impairments should be distributed among each node to maximize the PLS of the network? By defining the HI distribution factor $0 \leq \alpha \leq 1$, we provide some curves in Figure 12. Explicitly, this figure indicates that if a low number of relays is deployed, the highest secrecy rate is achieved when the relays experience equal HIs at the transmission and reception sections, i.e., $\alpha = 0.5$ for $\alpha\, K_R^t + (1-\alpha)\, K_R^r = 0.2$, and also the equipment used at the source and destination possess equal impairment values, i.e., $K_S^t = K_D^r = 0.1$. However, by increasing the number of relays, the network secrecy performance will be independent of the network HIs. This is because the network's degrees of freedom increases upon increasing the number of relays.

Finally, in Fig . 13, we aim for comparing the secrecy rate achieved by HJ policy with that of through the DACJ policy for different number of antennas deployed at the eavesdropper (i.e., Scheme 14,15). As it can be observed, the HJ policy outperforms the DACJ for $N_E = 1, 2$. However, for $N_E > 3$ the secrecy rate obtained through DACJ policy becomes higher than that of HJ policy. this is because of the fact that, although for $N_E > 3$ the external Eve will be actually the most curious node, the sub-optimal jammer found by HJ mechanism was relied upon the most curious nodes among untrusted relays whose CSI are known. It should be emphasized that, since in practice we have no knowledge about the number of antennas equipped at E, besides of the fact that the superiority of DACJ even in the case of $N_E > 3$ is negligible, the HJ policy is preferred rather than DACJ. However, with the aim of balancing between the secrecy performance gain and computational cost, the DACJ policy is more of interest.

VIII. Conclusions

In this article, we considered a cooperative relaying network including a source, a destination, a group of untrusted AF relays and an entirely passive multiple-antennas aided Eve, where all the legitimate nodes suffer from HIs. With the aim of safeguarding the confidential information against potential eavesdropping attacks, we proceed to boost the PLS of the network. To this end, we presented a novel joint cooperative beamforming, jamming and power allocation strategy to protect the confidential information while concurrently satisfying the required QoS at the destination. The corresponding optimization problem was divided into two consecutive sub-problems, where the first sub-problem was a non-convex problem and the second sub-problem was a convex one. For the non-convex problem, we proposed a low-complexity iterative algorithm to solve the DC program obtained, which relies on the CCCP. For this iterative algorithm, we also introduced a new initialization method which is based on a feasible point of the original problem. For the convex problem, we used the interior point method. For ease of exposition and make a sensible conclusion, the quantitative results are summarized in Table II.

Acknowledgment

This work was supported by the Iran National Science Foundation (INSF) under Grant No. 96014907.

Appendix

In this section, we establish a convergence analysis of DC programing. Since the original problem (30) is non-convex, it is not possible to prove convergence to the global minimum but rather to the *KKT* points under some regularity conditions. Recall that a feasible solution of (30) is regular if the set of gradients of active constraints at this point is linearly independent [35]. In general, the CCCP-based iterative algorithms converges to stationary point of DC programs [33]-[34], which are not necessarily local optima of DC programs. However, we prove that the proposed Algorithm 1 converges to one of its local minimum points of DC program (30). Our convergence proof is carried out in two steps. Specifically, 1) proof of convergence of Algorithm 1 to a stationary point, 2) proof that these stationary points are *KKT* points of problem (30). Before proceeding to prove convergence, we express the several important observations

- I. from (30), we observe that the objective function $\mathcal{D}_k(\boldsymbol{q}, \boldsymbol{v})$ is strictly decreasing in variables q_s and q_{J_1}.
- II. from (30-a) and (30-b), we observe that the $\mathcal{T}_k(\boldsymbol{q}, \boldsymbol{v})$ and $\mathcal{U}_k(\boldsymbol{q})$ are strictly increasing in variable q_s and strictly decreasing in the variable q_{J_1}.

TABLE II
Brief Review on Quantitative Results.

• The average convergence of the proposed FIPSA Algorithm is fast and it will be even faster, as the number of relays grows.
• Although the trusted relaying scenario provides better secrecy rate than untrusted relaying for small to medium total power budgets, upon increasing the total power budget, the secrecy performance of both the trusted and untrusted relaying converge a similar value.
• Given a specific total power budget, no matter what kind of relaying scenario (trusted or untrusted) is deployed, the achievable secrecy rate through our proposed method increases as the number of relays grows.
• The HJ mechanism outperforms the DACJ for small and moderate number of antennas employed at E. However, as the number of antennas grows, the DACJ policy results in a little better secrecy rate in compared with HJ. Nevertheless, since we have no knowledge about the number of antennas equipped at totally passive Eve, as well as the superiority of DACJ even in the case of large values of N_E is negligible, the HJ policy is preferred rather than DACJ. However, if we intend to balance between the secrecy performance gain and implementation cost, the DACJ policy is more of interest.
• Upon increasing the number of relays, while the secrecy rate of the DACJ policy is enhanced, not significant improvement is achieved through the HJ policy. Furthermore, particularly for medium and large amount of available total power budget, the HJ policy achieve a better secrecy rate.
• As the budget dedicated for jamming at Phase I increases, the communication becomes more robust against potent eavesdropping attack. Furthermore, more power should be assigned to convey the information signal.
• Upon increasing the level of HIs, the power required for information transmission is increased while the average secrecy rate is limited to a ceiling.
• The power $P_I + P_s$ we need for information transmission is decreased if the number of untrusted relays grows.
• If a low number of relays is deployed, the highest secrecy rate is achieved if the relays experience equal HIs at the transmission and reception sections and also the equipment used at the source and destination possess similar qualities. However, by increasing the number of relays, the network performance will be independent of the network HIs.

- III. from (32) and (33), we observed that the Taylor expansions (33-a) and (33-b) are strictly increasing and decreasing in the variables q_s and q_{J_1}, respectively.

Now we can analyze the convergence of the proposed Algorithm. The same analysis is applicable for the convergence behavior of FIPSA Algorithm. Note that, we assume that the initial point $\mathbf{t}^{(0)}$ is feasible. This assumption implies the feasibility of the entire points achieved by various iterations. Beck *et al* . in [58] proved that the solution of P_n obtained at the nth iteration $\mathbf{t}^{(n)}$ is a feasible solution of P_{n+1}. This fact implies that the corresponding objective value $\mathcal{D}_k(\mathbf{t}^{(n)})$ is not less than the optimal value of $\mathcal{D}_k(\mathbf{t}^{(n+1)})$. As a consequence, the sequence $\mathcal{D}_k(\mathbf{t}^{(n+1)})$ is not increasing, i.e., $\mathcal{D}_k(\mathbf{t}^{(n)}) > \mathcal{D}_k(\mathbf{t}^{(n+1)})$ as the iteration number n increases $(n \longrightarrow \infty)$. In addition, since the sequence $\mathcal{D}_k(\mathbf{t}^{(n)})$ is bounded below by zero and thus has a limit, so, the convergence of Algorithm 1 is guaranteed for any initial feasible point $\mathbf{t}^{(n)}$. Moreover, in section IV. A, we shown that the objective function $\mathcal{D}_k(\boldsymbol{t})$ of problem (34) is strictly convex in $\boldsymbol{t} \in R^{2\times 1} \bigotimes C^{(N-1)\times 1}$, i.e., the solution of problem (34), is unique [58].

According to a one-to-one relationship of the two sequences $\mathcal{D}_k(\mathbf{t}^{(n)})$ and $\mathbf{t}^{(n)}$ for any given initial feasible point $\mathbf{t}^{(0)}$, the monotone convergence of iterative sequence $\mathcal{D}_k(\mathbf{t}^{(n)})$ implies the convergence of $\mathbf{t}^{(n)}$ generated by CCCP method. Let $\boldsymbol{t}^*$ be an accumulation point of the sequence $\mathbf{t}^{(n)}$, we will show that $\boldsymbol{t}^*$ is a *KKT* point of problem (34), as well. Since $\boldsymbol{t}^*$ is an accumulation point of $\mathbf{t}^{(n)}$, there exist a subsequence $\mathbf{t}^{(k_n)}$ such that $\mathbf{t}^{(k_n)} \rightarrow \boldsymbol{t}^*$ when the iteration number n goes to infinity $(n \longrightarrow \infty)$. Regarding the limit point $\boldsymbol{t}^*$, we can make the following statement.

Lemma 3. *The accumulation point $\boldsymbol{t}^*$ of the sequence $\mathbf{t}^{(n)}$ generated by the proposed CCCP method is a KKT point of the following convex optimization problem:*

$$\mathbf{P}_3 : \ \min_{\mathbf{t}} \mathcal{D}_k(\mathbf{t}),$$

s.t.

$$\widehat{\mathcal{T}}_k(\mathbf{t}^{(n)}, \mathbf{t}) \triangleq \boldsymbol{\beta}_k\left(\mathbf{t}\right) - \widehat{\boldsymbol{\alpha}}\left(\mathbf{t}^{(n)}, \mathbf{t}\right) \leq 0, \qquad (a)$$

$$\widehat{\mho}_k(\mathbf{q}^{(n)}, \mathbf{q}) \triangleq \kappa\left(\mathbf{q}, \mu\right) - \widehat{\xi}\left(q_s^{(n)}, q_s\right) \leq 0, \qquad (b)$$

$$\mathcal{D}_k^{l,l}\left(\mathbf{t}\right) - Q_l \leq 0 \ , \ \forall l \in \mathcal{L}, \qquad (c)$$

$$\tfrac{1}{q_{J_1}} + \tfrac{1}{q_s} + \mathcal{D}_k\left(\mathbf{t}\right) - Q_{tot} \leq 0, \qquad (d)$$

$$\tfrac{1}{q_{J_1}} - \overline{P}_{J_1} \leq 0, \qquad (e)$$

$$\tfrac{1}{q_s} - P_T \leq 0. \qquad (f)$$

Proof: since the point $\mathbf{t^*} \triangleq \left[\mathbf{q^*}^T, \boldsymbol{v}^{*T}\right]^T$ is an accumulation point of the sequence $\mathbf{t}^{(n)}$, and the objective function $\mathcal{D}_k(\boldsymbol{t})$ of problem (33) is strictly convex in variable $\boldsymbol{t}$, so a unique solution can be achieved [33]. Therefore, the accumulation point $\boldsymbol{t}^*$ is the solution of problem (33). We use the contradiction method to show that constraints (33-a) and (33-b) should be active at the point $\boldsymbol{t}^*$, i.e., satisfy the equality at the point $\boldsymbol{t}^*$. Suppose that constraints (33-a) and (33-b) are not all active, i.e., some constraints satisfy with inequality at the $\mathbf{t^*} \triangleq \left[\mathbf{q^*}^T, \boldsymbol{v}^{*T}\right]^T$, for some $\alpha_1 > 0$ we can construct a feasible point $\tilde{\mathbf{t}}^* \triangleq \left[\left[a q_s^*, q_{J_1}^*\right]^T, \boldsymbol{v}^{*T}\right]^T$ without violating other constraints such that the constraints (33-a) and (33-b) are active and can achieve a lower objective value than that offered by $\boldsymbol{t}^*$, which leads to a contradiction. Therefore we can conclude that constraints (33-a) and (33-b) should be active at the accumulation point $\boldsymbol{t}^*$. ∎

We know from *lemma 3* that there exist Lagrangian multipliers $\{\lambda_i^*\}$ together with the accumulation point $\boldsymbol{t}^*$ that satisfy the following *KKT*'s necessary and sufficient condition for optimality of convex problem [35, Sec 5.5],

$$\begin{gathered}
\nabla\mathcal{D}_k(\boldsymbol{t}^*) + \lambda_1 \nabla\widehat{\mathcal{T}}_k(\boldsymbol{t}^*, \boldsymbol{t}^*) + \lambda_2 \nabla\widehat{\mho}_k(\boldsymbol{q}^*, \boldsymbol{q}^*) \\
+\lambda_3\left(\nabla\mathcal{D}_k^{(l,l)}(\boldsymbol{t}^*) - Q_l\right) + \lambda_4\left(\frac{1}{q_{J_1}^*} + \frac{1}{q_s^*} + \mathcal{D}_k(\boldsymbol{t}^*) - Q_{tot}\right) \\
+\lambda_5\left(\frac{1}{q_{J_1}^*} - \bar{P}_{J_1}\right) + \lambda_6\left(\frac{1}{q_s^*} - \bar{P}_T\right) = 0, \\
\mho_k(\boldsymbol{q}^*) = 0, \\
\mathcal{T}(\boldsymbol{t}^*) = 0,
\end{gathered}$$

From *lemma 3*, we proved that constraints (33-a) and (33-b) are active at the point $\boldsymbol{t}^*$, i.e. $\widehat{\mathcal{T}}_k(\boldsymbol{t}^*, \boldsymbol{t}^*) = \mathcal{T}(\boldsymbol{t}^*)$ and $\widehat{\mho}(\boldsymbol{q}^*, \boldsymbol{q}^*) = \mho_k(\boldsymbol{q}^*)$. Hence, the necessary *KKT* optimality conditions of (30) are given by following:

$$\begin{gathered}
\nabla\mathcal{D}_k(\boldsymbol{t}^*) + \gamma_1 \nabla\mathcal{T}(\boldsymbol{t}^*) + \gamma_2 \nabla\mho_k(\boldsymbol{q}^*) + \\
\gamma_3\left(\nabla\mathcal{D}_k^{(l,l)}(\boldsymbol{t}^*) - Q_l\right) + \\
\gamma_4\left(\frac{1}{q_{J_1}^*} + \frac{1}{q_s^*} + \mathcal{D}_k(\boldsymbol{t}^*) - Q_{tot}\right) + \\
\gamma_5\left(\frac{1}{q_{J_1}^*} - \bar{P}_{J_1}\right) + \gamma_6\left(\frac{1}{q_s^*} - \bar{P}_T\right) = 0,
\end{gathered}$$

where $\{\gamma_i\}_{i=1}^{6}$ denote the lagrangian multipliers of problem (30). If we choose$\gamma_i = \lambda_i, \forall i = 1, 2, \ldots, 6$, we conclude that the point $\boldsymbol{t}^*$ also satisfy So, we proved that if the sequence $\mathbf{t}^{(n)}$ generated by the CCCP method converges to a regular point $\boldsymbol{t}^*$, then $\boldsymbol{t}^*$ is a *KKT* point of the DC problem (30). Also it is easy to show that limit point $\boldsymbol{t}^*$ is a local minimum of the DC programming in (30). It has already been shown that the point $\boldsymbol{t}^*$ is a *KKT* point (stationary point) of the DC problem (30). This stationary point cannot be saddle point, since the objective function $\mathcal{D}_k(t)$ is strictly convex function and twice-continuously differentiable in the variable $\boldsymbol{t}$. By a simple contradiction method, we can also show that the point $\boldsymbol{t}^*$ cannot be a local maximum [58].

References

[1] Y. Liang, H. V. Poor, S. Shamai et al., “Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 45, pp. 355–580, 2009.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[4] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, “Physical layer security for the internet of things: authentication and key generation," *IEEE Wireless Communications*, 2019.

[5] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, “Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 3930–3941, 2016.

[6] 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 Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2015.

[7] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653–2661, 2013.

[8] Y. Zou, J. Zhu, X. Li, and L. Hanzo, “Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective," *IEEE Network*, vol. 30, no. 5, pp. 74–79, 2016.

[9] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, 2014.

[10] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, “Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks," *IEEE Access*, vol. 5, pp. 19620–19630, 2017.

[11] C. Wang, H.-M. Wang, and X.-G. Xia, “Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 589–605, 2014.

[12] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, “Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007–2020, 2013.

[13] H.-M. Wang, F. Liu, and M. Yang, “Joint cooperative beamforming, jamming, and power allocation to secure af relay systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4893–4898, 2015.

[14] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, “Cooperative secure beamforming for af relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.

[15] M. Luo, X. Li, J.Wang, Q. Yin,W. Tang, and S. Li, “Secure transmission schemes for two-way relay networks," *IEEE Access*, vol. 7, pp. 50148–50158, 2019.

[16] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, “Joint cooperative beamforming and jamming to secure af relay systems with individual power constraint and no eavesdropper?s csi," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 39–42, 2012.

[17] M. Moradikia, S. Mashdour, and A. Jamshidi, “Joint optimal power allocation, cooperative beamforming, and jammer selection design to secure untrusted relaying network," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 3, p. e3276, 2018.

[18] J. Yang, Q. Li, Y. Cai, Y. Zou, L. Hanzo, and B. Champagne, “Joint secure af relaying and artificial noise optimization: A penalized difference of convex programming framework," *IEEE Access*, vol. 4, pp. 10076–10095, 2016.

[19] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, “Secure transmissions in millimeter wave systems," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2114?2127, 2017.

[20] M. R. Khandaker and K.-K. Wong, “Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 40–54, 2014.

[21] N. Ouyang, X.-Q. Jiang, E. Bai, and H.-M. Wang, “Destination assisted jamming and beamforming for improving the security of af relay systems," *IEEE Access*, vol. 5, pp. 4125–4131, 2017.

[22] D. Chen, Y. Cheng, W. Yang, J. Hu, and Y. Cai, “Physical layer security in cognitive untrusted relay networks," *IEEE Access*, vol. 6, pp. 7055–7065, 2017.

[23] H. Zarrabi, A. Kuhestani, and M. Moradikia, “EE-rs and pa for untrusted relay network at high signal-to-noise ratio regime," *IET Communications*, vol. 10, no. 16, pp. 2143–2148, 2016.

[24] M. Atallah and G. Kaddoum, “Secrecy capacity scaling with untrustworthy aggressive relays cooperating with a wire-tapper," *IEEE Wireless Communications Letters,* vol. 5, no. 4, pp. 376–379, 2016.

[25] A. Kuhestani, A. Mohammadi, and M. Mohammadi, “Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 341–355, 2017.

[26] T. Schenk, *RF imperfections in high-rate wireless systems: impact and digital compensation*. Springer Science and Business Media, 2008.

[27] E. Bjornson, M. Matthaiou, and M. Debbah, “A new look at dualhop relaying: Performance limits with hardware impairments," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4512–4525, 2013.

[28] C. Studer, M. Wenk, and A. Burg, “MIMO transmission with residual transmit-Rf impairments," arXiv preprint arXiv:1002.0406, 2010.

[29] A.-A. A. Boulogeorgos, D. S. Karas, and G. K. Karagiannidis, “How much does i/q imbalance affect secrecy capacity?" *IEEE Communications Letters*, vol. 20, no. 7, pp. 1305–1308, 2016.

[30] A. Kuhestani, A. Mohammadi, K. Wong, P. L. Yeoh, M. Moradikia, and M. R. A. Khandaker, “Optimal power allocation by imperfect hardware analysis in untrusted relaying networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4302–4314, July 2018.

[31] H. A. Le Thi, “D.c. programming for solving a class of global optimization problems via reformulation by exact penalty," 2002, pp. 87–101.

[32] R. Horst and N. V. Thoai, “Dc programming: Overview," *Journal of Optimization Theory and Applications*, vol. 103, no. 1, pp. 1–43, Oct 1999. [Online]. Available: https://doi.org/10.1023/A:1021765131316

[33] A. L. Yuille and A. Rangarajan, “The concave-convex procedure," *Neural Computation*, vol. 15, no. 4, pp. 915–936, 2003. [Online]. Available: https://doi.org/10.1162/08997660360581958

[34] G. R. Lanckriet and B. K. Sriperumbudur, “On the convergence of the concave-convex procedure," in Advances in *Neural Information Processing Systems* 22, Y. Bengio, D. Schuurmans, J. D. Lafferty, C. K. I. Williams, and A. Culotta, Eds. Curran Associates, Inc., 2009, pp. 1759–1767. [Online]. Available: http://papers.nips.cc/paper/ 3646-on-the-convergence-of-the-concave-convex-procedure.pdf

[35] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge University Press, 2004.

[36] D. H. Brandwood, “A complex gradient operator and its application in adaptive array theory," *IEE Proceedings H - Microwaves, Optics and Antennas*, vol. 130, no. 1, pp. 11–16, February 1983.

[37] C. D?ambrosio, A. Frangioni, L. Liberti, and A. Lodi, “A storm of feasibility pumps for nonconvex minlp," *Math. Program.*, vol. 136, no. 2, pp. 375–402, Dec. 2012. [Online]. Available: https://doi.org/10.1007/s10107-012-0608-x

[38] N. Bornhorst, M. Pesavento, and A. B. Gershman, “Distributed beamforming for multi-group multicasting relay networks," *Trans. Sig. Proc.*, vol. 60, no. 1, pp. 221–232, Jan. 2012. [Online]. Available: https://doi.org/10.1109/TSP.2011.2167618

[39] C. E. Shannon, “Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[40] A. D. Wyner, “The wire-tap channel," *Bell system technical journal,* vol. 54, no. 8, pp. 1355–1387, 1975.

[41] I. Csiszar and J. Korner, “Broadcast channels with confidential messages," *IEEE Transactions on Information Theory,* vol. 24, no. 3, pp. 339–348, May 1978.

[42] S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[43] Y. Oohama, “Coding for relay channels with confidential messages," in *Proceedings 2001 IEEE Information Theory Workshop* (Cat. No.01EX494), Sep. 2001, pp. 87–89.

[44] X. He and A. Yener, “Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, Nov 2008, pp. 1–5.

[45] X. He and A. Yener, “Cooperation with an untrusted relay: A secrecy perspective," arXiv preprint arXiv:0910.1511, 2009.

[46] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[47] J. Li, A. P. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, Oct 2011.

[48] J. Huang and A. L. Swindlehurst, “Cooperative jamming for secure communications in mimo relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct 2011.

[49] C. Jeong, I. Kim, and D. I. Kim, “Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, Jan 2012.

[50] J. Mo, M. Tao, Y. Liu, and R. Wang, “Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Transactions on Signal Processing*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[51] C. Wang and H.-M. Wang, “Robust joint beamforming and jamming for secure af networks: Low-complexity design," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 2192–2198, 2014.

[52] J. Xiong, L. Cheng, D. Ma, and J. Wei, “Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7274–7284, Sep. 2016.

[53] J. Zhu, R. Schober, and V. K. Bhargava, “Physical layer security for massive MIMO systems impaired by phase noise," in *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, July 2016, pp. 1–5.

[54] B. Ali, N. Zamir, M. Fasih, U. Butt, and S. X. Ng, “Physical layer security: Friendly jamming in an untrusted relay scenario," in *2016 24th European Signal Processing Conference (EUSIPCO)*, Aug 2016, pp. 958–962.

[55] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, “Analysis and design of secure massive mimo systems in the presence of hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2001–2016, Mar. 2017.

[56] Q. Li and L. Yang, “Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2628–2638, Oct. 2018.

[57] T. Mekkawy, R. Yao, T. A. Tsiftsis, F. Xu, and Y. Lu, “Joint beamforming alignment with suboptimal power allocation for a two-way untrusted relay network," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2464–2474, Oct. 2018.

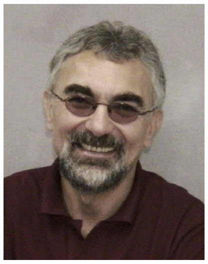
[58] A. Beck, A. Ben-Tal, and L. Tetruashvili, “A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *Journal of Global Optimization*, vol. 47, no. 1, pp. 29–51, May 2010. [Online]. Available: https://doi.org/10.1007/s10898-009-9456-5

Majid Moradikia was born in 1986. He received the Ph.D. degree in Telecommunication system engineering at the Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran. He currently works as research assistant at the Electrical Engineering Department, Sharif University of Technology, Tehran, Iran. His main research interests lie within the area of physical-layer security of wireless communications, Internet of Things, millimeter-wave communication systems, massive MIMO systems.

Hamed Bastami received the M.Sc. degree in Electrical Engineering from the University of Tehran, Tehran, Iran, in 2014. He is currently a Ph.D. student with the Department of Electrical Engineering, Sharif University of Technology, under the supervision of Dr. Behroozi. His research interests lie in the areas of physical-layer security (PLS) of wireless communications with special emphasis on machine learning, deep-based PLS in wireless communication and unmanned areal vehicle (UAV) networks.

Ali Kuhestani received his Ph.D. degree in Electrical Engineering from the Amirkabir University of Technology, Tehran, Iran, in 2017. Since 2018, he has been a Post-Doctoral Researcher with the Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran. He has authored and coauthored more than 15 journals in prestigious publication avenues (e.g., the IEEE and IET) and about 10 papers in major conference proceedings. His research interests include physical-layer security of wireless communications, Internet of Things, millimeter-wave communication, massive MIMO system, and space-time coding. He was a reviewer of the IEEE transactions/journals and conferences. He was the recipient of Iran’s National Elites Foundation Award for outstanding students in 2017.

Hamid Behroozi (S’04-M’08) received the B.Sc. degree in Electrical Engineering from the University of Tehran, Tehran, Iran, in 2000, the M.Sc. degree in Electrical Engineering from Sharif University of Technology, Tehran, in 2003, and the Ph.D. degree in Electrical Engineering from Concordia University, Montreal, QC, Canada, in 2007. From 2007 to 2010, he was a Postdoctoral Fellow with the Department of Mathematics and Statistics, Queens University, Kingston, ON, Canada. He is currently an Associate Professor with the Department of Electrical Engineering, Sharif University of Technology, Tehran. His research interests include information theory, joint source-channel coding, artificial intelligence in signal processing and data science, and cooperative communications. Dr. Behroozi was the recipient of several academic awards, including Ontario Postdoctoral Fellowship awarded by the Ontario Ministry of Research and Innovation (MRI), Quebec Doctoral Research Scholarship awarded by the Government of Quebec (FQRNT), Hydro Quebec Graduate Award, and Concordia University Graduate Fellowship.



Lajos Hanzo FREng, F’04, FIET, Fellow of EURASIP, received his 5-year degree in electronics in 1976 and his doctorate in 1983 from the Technical University of Budapest. In 2009 he was awarded an honorary doctorate by the Technical University of Budapest and in 2015 by the University of Edinburgh. In 2016 he was admitted to the Hungarian Academy of Science. During his 40-year career in telecommunications he has held various research and academic posts in Hungary, Germany and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised 119 PhD students, co-authored 18 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1800+ research contributions at IEEE Xplore, acted both as TPC and General Chair of IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. Currently he is directing a 60-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Council’s Advanced Fellow Grant and the Royal Society’s Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses. He is also a Governor of the IEEE ComSoc and VTS. He is a former Editor-in-Chief of the IEEE Press and a former Chaired Professor also at Tsinghua University, Beijing. For further information on research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk