This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

Joint Beamforming and Power Allocation for Secrecy in Peer-to-Peer Relay Networks

Chao Wang, Hui-Ming Wang, *Member, IEEE*, Derrick Wing Kwan Ng, *Member, IEEE*, Xiang-Gen Xia, *Fellow, IEEE*, and Chaowen Liu

***Abstract*—This paper investigates the physical-layer security of a multiuser peer-to-peer (MUP2P) relay network for amplify-and-forward (AF) protocol, where a secure user and other unclassified users coexist with a multi-antenna eavesdropper and the eavesdropper can wiretap the confidential information in both two cooperative phases. Our goal is to optimize the transmit power of the source and the beamforming weights of the relays jointly for secrecy rate maximization subject to the minimum signal-to-interference-noise-ratio (SINR) constraint at each user, and the individual and total power constraints. Mathematically, the optimization problem is non-linear and non-convex, which does not facilitate an efficient resource allocation algorithm design. As an alternative, a null space beamforming scheme is adopted at the relays for simplifying the joint optimization and eliminating the confidential information leakage in the second cooperative phase, where the relay beamforming vector lies in the null space of the equivalent channel of the relay to eavesdropper links. Although the null space beamforming scheme simplifies the design of resource allocation algorithm, the considered problem is still non-convex and obtaining the global optimum is very difficult, if not impossible. Employing a sequential parametric convex approximation (SPCA) method, we propose an iterative algorithm to obtain an efficient solution of the non-convex problem. Besides, the proposed joint design algorithm requires a feasible starting point, we also propose a low complexity feasible initial points searching algorithm. Simulations demonstrate the validity of the proposed strategy.**

***Index Terms*—Multiuser peer-to-peer relay network, secrecy rate maximization, sequential parametric convex approximation, feasible initial points searching algorithm.**

I. Introduction

THE security and privacy are the fundamental problems in data transmission. They have become more challenging in the *wireless* communications due to the broadcast nature of the wireless medium. Following the pioneering work in [1], which introduced the wiretap model and defined the concept of secrecy capacity, massive works have investigated the security problem on the physical layer from an information-theoretic perspective [2]-[5]. It has been shown that multiple-input multiple-output (MIMO) technique has a great potential to enhance the security of wireless data transmissions [6]-[8]. The secrecy capacity of a multiple-input, single-output, multi-eavesdropper (MISOME) wiretap channel has been investigated in [6], and the optimal solutions for the MIMO Gaussian wiretap channel were studied in [7], [8]. Recently, the security issues in the downlink of a mobile wireless system have received the increasing attention. Assuming that base station (BS) has multiple antenna elements while all legitimate nodes and the eavesdroppers are equipped with a single antenna, the authors in [9] optimize the linear precoder for the secrecy rate maximization in multiuser multiple antennas wireless networks. The physical layer security issue in multibeam satellite systems has been addressed in [10]. In [11], we proposed a secure multiple-antenna transmission scheme for the cognitive radio network in slow fading channels. A survey of the recent advances on this topic can be found in [12]. However, due to the cost and size limitations, it is difficult to deploy the multiple antennas at some network nodes, e.g., handheld devices and sensors. As a result, the idea of cooperative communication has been considered as a viable solution for providing secure transmission for portable devices.

Cooperative beamforming (CB) and cooperative jamming (CJ) are two strategies which can be adopted by the cooperative nodes to enhance the security. The security issues of the amplify-and-forward (AF) and decode-and-forward (DF) one-way relay networks have been discussed with details in [13]-[17], where beamformer and power allocations are optimized to maximize the achievable secrecy rate of the transmission. However, it has been shown that the problem is non-convex, and obtaining the optimal solution may require prohibitively high computational complexity. Therefore, some suboptimal schemes are proposed, such as null space beamforming. When the channel state information (CSI) can be only known imperfectly, robust CB and CJ design schemes in the presence of multiple multi-antenna eavesdroppers have been proposed in [15]. Similar problems have also been investigated in two-way relay networks [18],[19]. Compared with CB, the opportunistic relay selection (ORS) is a low overhead alternative by selecting a single relay to forward the desired signals while retaining the diversity gain achieved by CB [20]. In [21], [22], the ORS has been adopted to improve the

The work of C. Wang, H.-M. Wang and C. Liu was partially supported by the NSFC under Grants No. 61102081, and No. 61221063, the Foundation for the Author of National Excellent Doctoral Dissertation of China under Grant 201340, the New Century Excellent Talents Support Fund of China under Grant NCET-13-0458, the Fok Ying Tong Education Foundation under Grant 141063, and the Fundamental Research Funds for the Central University under Grant No. 2013jdgz11. The work of D. W. K. Ng was partially supported by the AvH Professorship Program of the Alexander von Humboldt Foundation.

C. Wang, H.-M. Wang and C. Liu are with the School of Electronic and Information Engineering, and also with the MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, China. Email: wangchaoxuzhou@stu.xjtu.edu.cn, xjbswhm@gmail.com, liucwhb@gmail.com. H.-M. Wang is the corresponding author.

D. W. K. Ng is with the Institute for Digital Communications (IDC), Friedrich-Alexander-University Erlangen-Nürnberg (FAU), 91058 Erlangen, Germany. Email: kwan@lnt.de.

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, USA. Email: xxia@ee.udel.edu.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

wireless security against eavesdropping. To further improve the security, hybrid beamforming/opportunistic relaying and jamming schemes have been proposed for both one- and two-way relay networks in [23]-[25], where both two phases of the cooperative transmissions will be under protection. In [26], modeling the positions of jammers and eavesdroppers by two-dimensional homogeneous Poisson point processes, we proposed an opportunistic jammer selection approach for protecting the confidential information transmission.

All the above works only consider a single source-destination pair. For improving the spectrum efficiency of the cooperative communication, multiuser peer-to-peer (MUP2P) relay networks is proposed in [27], where multiple source-destination pairs communicate in a pairwise manner with the help of multiple relay nodes. Recently, MUP2P relay networks under AF relaying have been receiving increasing attention [28]-[30]. In MUP2P2 relay networks, the concurrent transmission of multiple users may result in harmful co-channel interference. But for guaranteeing the secrecy of the system, the concurrent transmission of multiple users may benefit the secure transmission [31] when the transmission is carefully designed. Therefore, how to coordinate the concurrent transmission of multiple users for maximizing the achievable secrecy rate in MUP2P relay networks is a very interesting problem. However, to the best knowledge of the authors, none of the prior works has addressed this problem.

In this paper, we study the security issue of a MUP2P relay network, where a secure user transmits a confidential information to its intended destination in the presence of a multi-antenna eavesdropper, and the other unclassified users transmit the information without secrecy requirement. Since the eavesdropper is only interested in the confidential information transmitted from the secure user, the concurrent data transmission of the unclassified users may be considered as "jamming signals" for the eavesdropper which benefits the secure transmission [9], [31]. In other words, the signals transmitted from the unclassified users can be exploited to protect the confidential information from eavesdropping by interfering with the eavesdropper. Since the eavesdropper can wiretap the confidential information during two cooperative phases, we jointly design the transmit power of the source and beamformer of the relays to maximize the secrecy rate of the secure user under some Quality of Service (QoS) constraints, i.e., the received signal-to-interference-plus-noise ratio (SINR) requirement at each destination should be satisfied. Mathematically, the optimization problem obtained is non-linear and non-convex, which is very difficult to solve, if not impossible. As an alternative, the null space beamforming is employed by the relay nodes to eliminate the confidential information leakage in the second cooperative phase, which results in a simpler non-convex optimization problem. To strike a balance between computational complexity and optimality, we adopt the sequential parametric convex approximation (SPCA) method [39], [40] to obtain an efficient solution of the considered non-convex optimization problem. SPCA is an efficient iterative approach for handling the non-convex problem. With SPCA, the non-convex feasible set of a non-convex optimization problem is approximated by an appropriate inner convex feasible set at each iteration and the approximation is improved over iterations. Then, an efficient solution of the non-convex problem can be obtained by solving a series of convex programs.

Overall, our contributions can be summarized as follows:

1) We propose a joint design approach for maximizing the achievable secrecy rate in AF MUP2P relay networks, where the transmit power of multiple sources and the relay beamformer are designed jointly. Although the resulting problem is non-convex, employing SPCA [39], [40], we approximate the non-convex problem by a sequence of convex approximation problems and obtain an efficient solution.
2) To solve the joint optimization problem, an initial point of SPCA should be feasible to the original problem [40]. However, the task in calculating feasible points of a non-convex optimization problem is NP-hard in general [32]. In order to handle this problem, we propose an initialization procedure which solves the feasibility problem iteratively. The proposed initialization procedure can also be applied to get the feasible initial point when adopting SPCA to solve other non-convex problems [40].

Notation: $(.)^T$, $(.)^*$, and $(.)^H$ denote the transpose, conjugate, and conjugate transpose, respectively. $(.)^{-1}$ denotes the inverse of a matrix. $\Re(.)$ and $\Im(.)$ denote the real and imaginary part of a variable, respectively. $\mathbb{E}(.)$ denotes the expectation. $\mathbb{R}_+^{L\times 1}$ denotes the set of positive real L-vector, $\mathbb{C}^{L\times 1}$ denotes the set of complex L-vector, $\mathbb{C}^{n\times n}$ stands for an $n\times n$ complex matrix. $\mathbf{I}_N$ denotes $N\times N$ identity matrix, $\mathbf{e}_i$ is an unit vector with the ith entry equals to one, diag($\mathbf{a}$) is the diagonal matrix with $\mathbf{a}$ on its main diagonal, $\mathbf{E}_i \triangleq \text{diag}(\mathbf{e}_i)$, and $\mathbf{x} \sim \mathcal{CN}(\mathbf{\Lambda}, \mathbf{\Delta})$ is denoted as the circular symmetric complex Gaussian vector with mean vector $\mathbf{\Lambda}$ and covariance matrix $\mathbf{\Delta}$. $\mathbf{X} \succeq \mathbf{0}$ represents that $\mathbf{X}$ is a Hermitian positive semidefinite matrix. $[x]^+ \triangleq \max(x, 0)$.

II. System Model

The AF MUP2P relay network illustrated in Fig.1 is considered, which consists of K sources $\{S_i\}_{i=1}^K$, K destinations $\{D_i\}_{i=1}^K$, L trusted relay nodes $\{R_i\}_{i=1}^L$, and a multi-antenna eavesdropper, Eve[1]. We assume that S_{k^*} is the secure user which transmits the confidential information to its intended receiver D_{k^*}, while the confidential information is eavesdropped by Eve. Besides user S_{k^*}, the other sources are unclassified users sending informations without the requirement of communication security. Eve is equipped with N_E antennas, while all the other nodes are single-antenna devices. We assume that the relays are closed to each other and form an AF cooperative cluster [37] so as to help the sources to convey information to their intended destinations, i.e., $S_i \rightarrow D_i$. In this paper, we also assume that $L \geq K + N_E$ for guaranteeing communication security. Besides, we focus on quasi-stationary flat-fading channels.

[1]A multiple-antenna eavesdropper can be regarded as multiple colluding eavesdroppers, which share their antennas and perform joint processing to form a super eavesdropper.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

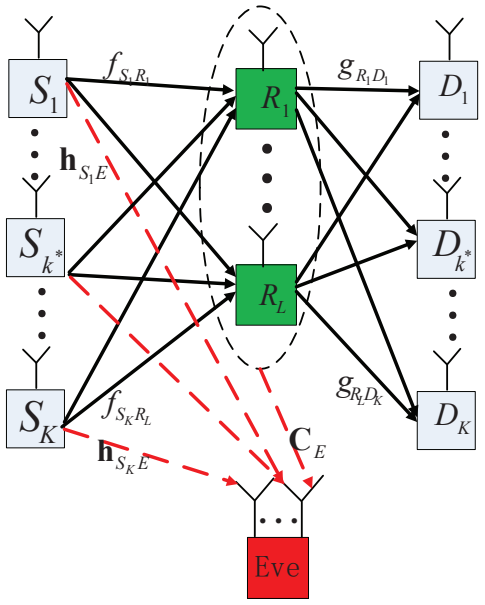

Fig. 1. The multiuser peer-to-peer relay network with a multi-antenna eavesdropper.

Assuming that there is no direct link between the sources and destinations due to heavy blockage and all the nodes operate in the half-duplex mode, the two-hop data transmission takes place in two consecutive time-slots. Therefore, Eve can wiretap the confidential information in both the two cooperative phases: from S_{k^*} to the relays and from the relays to the destinations.

In Phase I, the received signal vectors at the relay nodes, $\mathbf{y}_R$, and Eve, $\mathbf{y}_{E,1}$, are given as follows

$$\mathbf{y}_R = [y_{R,1}, \ldots, y_{R,L}]^T = \sum_{k=1}^{K} \mathbf{f}_{S_kR} \sqrt{P_k} x_k + \mathbf{n}_R, \tag{1}$$

$$\mathbf{y}_{E,1} = \mathbf{h}_{S_{k^*}E} \sqrt{P_{k^*}} x_{k^*} + \underbrace{\sum_{i=1, i\neq k^*}^{K} \mathbf{h}_{S_iE} \sqrt{P_i} x_i}_{\text{interference}} + \mathbf{n}_{E,1}, \tag{2}$$

where

a) vector $\mathbf{f}_{S_kR} \triangleq [f_{S_kR_1}, \ldots, f_{S_kR_L}]^T \in \mathbb{C}^{L\times 1}$, with $f_{S_kR_l}$ denoting the complex valued channel coefficient from the kth source to the lth relay, $\forall k \in \mathcal{K}$, $\forall l \in \mathcal{L}$, with $\mathcal{K} \triangleq \{1, \ldots, K\}$ and $\mathcal{L} \triangleq \{1, \ldots, L\}$;

b) vector $\mathbf{h}_{S_kE} \in \mathbb{C}^{N_E\times 1}$ denotes the channel vector from the kth source to Eve, $\forall k \in \mathcal{K}$;

c) vector $\mathbf{P} \triangleq [P_1, \ldots, P_K]^T \in \mathbb{R}_+^{L\times 1}$, with P_k denoting the transmit power of the kth source that should satisfy the individual power constraints: $P_k \leq P_{S_k}$, $\forall k \in \mathcal{K}$, where P_{S_k} is the transmit power budget at S_k;

d) $\mathbf{x} \triangleq [x_1, \ldots, x_K]^T$, where variable x_k is the transmitted signal at S_k and $\mathbb{E}(\mathbf{x}\mathbf{x}^H) = \mathbf{I}_K$;

e) vector $\mathbf{n}_R \triangleq [n_{R,1}, \ldots, n_{R,L}]^T \in \mathbb{C}^{L\times 1}$, with $n_{R,l} \sim \mathcal{CN}(0, \sigma^2)$ denoting the additive white Gaussian noise (AWGN) at the lth relay. $\mathbf{n}_{E,1} \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_{N_E})$ denotes the AWGN at Eve in Phase I.

Since the transmitted signals for the K users from the sources are independent, the signals from unclassified users are treated as interference at Eve, which can weaken the wiretap capability of Eve. As a result, multiuser transmission benefits the communication in the sense of security [10], [31], [33], [34].

In Phase II, the relay nodes amplify and forward their received signals to the destinations. The received signals at the kth destination and Eve are given as follows

$$y_k = \mathbf{g}_{RD_k}^T \mathbf{W}^H \mathbf{y}_R + n_k, \tag{3}$$

$$\mathbf{y}_{E,2} = \mathbf{C}_E \mathbf{W}^H \mathbf{y}_R + \mathbf{n}_{E,2}, \tag{4}$$

f) matrix $\mathbf{W}^H \triangleq \text{diag}\{\mathbf{w}^*\}$, with the beamformer $\mathbf{w}^* \triangleq [w_1^*, \ldots, w_L^*]^T \in \mathbb{C}^{L\times 1}$ and w_l^* denotes the beamforming weight adopted by the lth relay;

g) vector $\mathbf{g}_{RD_k} \triangleq [g_{R_1D_k}, \ldots, g_{R_LD_k}]^T \in \mathbb{C}^{L\times 1}$, with $g_{R_lD_k}$ denoting the channel coefficient from the lth relay to the kth destination, $\forall l \in \mathcal{L}, \forall k \in \mathcal{K}$;

h) matrix $\mathbf{C}_E \in \mathbb{C}^{N_E\times L}$ denotes the channel from the relays to Eve;

i) $n_k \sim \mathcal{CN}(0, \sigma^2)$ denotes the AWGN at the kth destination and $\mathbf{n}_{E,2} \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_{N_E})$ denotes the AWGN at Eve in Phase II.

The transmitted signals from the relays, $\mathbf{W}^H\mathbf{y}_R$ should satisfy both the individual power constraint at each relay and the total power constraint:

$$\sum_{k=1}^{K} P_k \mathbf{w}^H \mathbf{F}_k \mathbf{e}_l \mathbf{e}_l^H \mathbf{F}_k^H \mathbf{w} + \mathbf{w}^H \mathbf{E}_l \mathbf{w} \sigma^2 \leq Q_l, \quad \forall l \in \mathcal{L}, \tag{5}$$

$$\sum_{k=1}^{K} P_k + \sum_{k=1}^{K} P_k \mathbf{w}^H \mathbf{F}_k \mathbf{F}_k^H \mathbf{w} + \mathbf{w}^H \mathbf{w} \sigma^2 \leq Q_{tot}, \tag{6}$$

where $\mathbf{F}_k \triangleq \text{diag}\{\mathbf{f}_{S_kR}\}$ denotes a diagonal matrix, 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 for the whole network due to the spectrum mask constraint.

Substituting (1) into (3) and (4), we obtain the end-to-end input-output relationship of the source-destination pair, $S_k \to D_k$ and the source-relay-Eve, $S_{k^*} \to R \to E$, as follows

$$y_k = \mathbf{w}^H \mathbf{G}_k \mathbf{f}_{S_kR} \sqrt{P_k} x_k + \underbrace{\sum_{i=1, i\neq k}^{K} \mathbf{w}^H \mathbf{G}_k \mathbf{f}_{S_iR} \sqrt{P_i} x_i}_{\text{CCI}} + \mathbf{w}^H \mathbf{G}_k \mathbf{n}_R + n_k, \tag{7}$$

$$\mathbf{y}_{E,2} = \mathbf{C}_E \mathbf{F}_{k^*} \mathbf{w}^* \sqrt{P_{k^*}} x_{k^*} + \underbrace{\sum_{i=1, i\neq k^*}^{K} \mathbf{C}_E \mathbf{F}_i \mathbf{w}^* \sqrt{P_i} x_i}_{\text{interference}} + \mathbf{C}_E \mathbf{W}^H \mathbf{n}_R + \mathbf{n}_{E,2}, \tag{8}$$

where $\mathbf{G}_k \triangleq \text{diag}\{\mathbf{g}_{RD_k}\}$, $\forall k \in \mathcal{K}$. The destinations are assumed to perform single user detection, therefore, the co-channel interference (CCI) at each destination is treated as noise. Combining (2) and (8) yields the receive model of the eavesdropper in the two transmission phases as

$$\mathbf{y}_E = \mathbf{H}_E x_{k^*} + \mathbf{n}_E, \tag{9}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

where

$$\mathbf{y}_E = \begin{bmatrix} \mathbf{y}_{E,1} \\ \mathbf{y}_{E,2} \end{bmatrix}, \mathbf{H}_E = \begin{bmatrix} \mathbf{h}_{S_{k^*}E}\sqrt{P_{k^*}} \\ \mathbf{C}_E\mathbf{F}_{k^*}\mathbf{w}^*\sqrt{P_{k^*}} \end{bmatrix},$$
$$\mathbf{n}_E = \begin{bmatrix} \sum_{i=1,i\neq k^*}^{K} \mathbf{h}_{S_iE}\sqrt{P_i}x_i + \mathbf{n}_{E,1} \\ \sum_{i=1,i\neq k^*}^{K} \mathbf{C}_E\mathbf{F}_i\mathbf{w}^*\sqrt{P_i}x_i + \mathbf{C}_E\mathbf{W}^H\mathbf{n}_R + \mathbf{n}_{E,2} \end{bmatrix}, \tag{10}$$

and $\mathbf{n}_E$ is zero-mean Gaussian vector with covariance matrix $\mathbf{Q}_E$ which is given in (11) at the top of the next page.

From the equations above, we have the following observations:

1) for each legitimate terminal, the equivalent channel model is single-input single-output (SISO) as described in (7).
2) for the eavesdropper, two transmission phases offer two opportunities to wiretap the information. This implies the optimal strategy adopted by the eavesdropper is to combine the information received over the two phases.

As shown in [13], [18], [19], using Gaussian inputs and stochastic encoders, the achievable secrecy rate of S_{k^*} can be calculated by

$$R_s = \left[I(y_{k^*}; x_{k^*}) - I(\mathbf{y}_E; x_{k^*})\right]^+, \tag{12}$$

where $I(.;.)$ is the mutual information.

The information rate achieved by the legitimate terminal over the two phases is given by (13) at the top of the next page. The factor $1/2$ results from the required two time slots for the whole transmission due to the half-duplex relaying mode.

On the other hand, the information rate leaked to the eavesdropper can be quantified by the sum rate of the MIMO system (9) which is given by

$$R_E \triangleq I(\mathbf{y}_E; x_{k^*}) = \frac{1}{2}\log_2\left(\det\left(\mathbf{I}_{2N_E} + \mathbf{H}_E\mathbf{H}_E^H\mathbf{Q}_E^{-1}\right)\right). \tag{14}$$

Substituting (13) and (14) into (12) yields the achievable secrecy rate R_s which is given by (15) at the top of the next page

The achievable secrecy rate in (15) is a nonlinear and non-convex function of $\mathbf{w}$ and $\mathbf{P}$ which leads to an intractable joint beamforming and power allocation design. Furthermore, the two transmission phases result in two opportunities in information leaked to Eve, which makes the system vulnerable to eavesdropping. As a countermeasure, the "Null Space Beamforming" is adopted to completely eliminate the information leakage in Phase II and to facilitate the joint design. Specifically, we adopt $\mathbf{w}^*$ such that it lies in the null space of the equivalent channel of the relay link from S_{k^*} to Eve, i.e., $\mathbf{C}_E\mathbf{F}_{k^*}\mathbf{w}^* = \mathbf{0}$, where $\mathbf{w}^*$ can be chosen as $\mathbf{w}^* = \mathbf{U}^T\mathbf{v}^*$, matrix $\mathbf{U}^T$ denotes the column-orthogonal matrix corresponding to the null space of the matrix $\mathbf{C}_E\mathbf{F}_{k^*}$, and $\mathbf{v}^*$ is an arbitrary vector with dimension $(L-N_E)\times 1$, which would be optimized for maximizing the achievable secrecy performance in the next section. At Eve, the confidential signals transmitted by all the relays are completely nulled out, while only the mixed signals from multiuser in Phase I are received. Therefore, the wiretap capability of Eve is determined by the information leakage in Phase I, i.e., (2). Although with the null space beamforming, the relay has lost some degrees of freedoms to null out the confidential signals at Eve, the null space beamforming still benefits the secrecy performance of the relay network. Since with the null space beamforming, the degradation of the reception quality at Eve is more serious than the one at the secure destination, and the achievable secrecy performance is determined by the difference of the reception quality of the legitimate node and eavesdropper cf. eq. (15), we expect that the null space beamforming would improve the achievable secrecy performance of the relay network. Furthermore, as shown in [17], the null space beamforming design approaches the optimal design in AF relay networks in high SNR regime. Recently, the null space beamforming method has been adopted in [18], [19] for securing the two-way relaying networks. In this paper, just as [13], [14], [28]-[30], the global CSIs are assumed to be available at a control center which designs $\mathbf{w}^*$ and the power allocation vector $\mathbf{P}$ jointly. The global CSIs can be obtained with the CSIs feedback from the relay nodes to the control center.

Remark 1: In this work, the instantaneous CSIs of the eavesdropper are assumed to be available, which has been widely adopted in the literatures for designing the secure transmission schemes [9], [10], [13], [18], [19], [14], [22], [35]. This assumption is applicable in networks combining broadcast and multicast transmissions [9], in which the destinations play dual roles as legitimate users for some signals and eavesdroppers for others. Furthermore, a recent research has shown that even for a passive eavesdropper, we can still estimate the channel state information (CSI) through the local oscillator power inadvertently leaked from the eavesdroppers receiver RF frontend [36].

.

III. Joint Power Allocation and CB Design for Secrecy Rate Maximization

In this section, we derive a SPCA-based optimization approach for maximizing the achievable secrecy rate subject to QoS, individual, and total power constraints.

A. Problem Formulation

The problem of interest is to maximize the secrecy rate achieved by the secure user S_{k^*} while maintaining a minimum QoS level for each source-destination pair. Similar to [28], [29], [30], for the K source-destination pairs, we define the following QoS constraints

$$\gamma_k(\mathbf{v}, \mathbf{P}) \geq \gamma_k^{\min}, \quad \forall k \in \mathcal{K}, \tag{16}$$

where

$$\gamma_k(\mathbf{v}, \mathbf{P}) = \frac{P_k\mathbf{v}^H\mathbf{\Psi}_{k,k}\mathbf{v}}{\sum_{i=1,i\neq k^*}^{K} P_i\mathbf{v}^H\mathbf{\Psi}_{k,i}\mathbf{v} + \mathbf{v}^H\mathbf{\Omega}_k\mathbf{v}\sigma^2 + \sigma^2}, \tag{17}$$

is the achievable SINR at D_k, $\mathbf{\Psi}_{k,i} \triangleq \mathbf{U}\mathbf{G}_k\mathbf{f}_{S_iR}\mathbf{f}_{S_iR}^H\mathbf{G}_k^H\mathbf{U}^H$, $\mathbf{\Omega}_k \triangleq \mathbf{U}\mathbf{G}_k\mathbf{G}_k^H\mathbf{U}^H$, and $\gamma_k^{\min}$ is the predefined received SINR threshold at D_k.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

$$\mathbf{Q}_E = \begin{bmatrix} \sum_{i=1,i\neq k^*}^{K} P_i \mathbf{h}_{S_i E}\mathbf{h}_{S_i E}^H + \sigma^2 \mathbf{I}_{N_E} & \sum_{i=1,i\neq k^*}^{K} P_i \mathbf{h}_{S_i E}\mathbf{w}^T \mathbf{F}_i^H \mathbf{C}_E^H \\ \sum_{i=1,i\neq k^*}^{K} P_i \mathbf{C}_E \mathbf{F}_i \mathbf{w}^* \mathbf{h}_{S_i E}^H & \sum_{i=1,i\neq k^*}^{K} P_i \mathbf{C}_E \mathbf{F}_i \mathbf{w}^* \mathbf{w}^T \mathbf{F}_i^H \mathbf{C}_E^H + \sigma^2 \mathbf{C}_E \mathbf{W}^H \mathbf{W} \mathbf{C}_E^H + \sigma^2 \mathbf{I}_{N_E} \end{bmatrix}. \tag{11}$$

$$R_{k^*} \triangleq I(y_{k^*}; x_{k^*}) = \frac{1}{2}\log_2 \left(1 + \frac{P_{k^*} \mathbf{w}^H \mathbf{G}_{k^*} \mathbf{f}_{S_{k^*}R} \mathbf{f}_{S_{k^*}R}^H \mathbf{G}_{k^*}^H \mathbf{w}}{\sum_{i=1,i\neq k^*}^{K} P_i \mathbf{w}^H \mathbf{G}_{k^*} \mathbf{f}_{S_i R} \mathbf{f}_{S_i R}^H \mathbf{G}_{k^*}^H \mathbf{w} + \mathbf{w}^H \mathbf{G}_{k^*} \mathbf{G}_{k^*}^H \mathbf{w} \sigma^2 + \sigma^2} \right). \tag{13}$$

$$R_s = [R_{k^*} - R_E]^+ = \left[\frac{1}{2}\log_2 \left(\frac{1 + \frac{P_{k^*} \mathbf{w}^H \mathbf{G}_{k^*} \mathbf{f}_{S_{k^*}R} \mathbf{f}_{S_{k^*}R}^H \mathbf{G}_{k^*}^H \mathbf{w}}{\sum_{i=1,i\neq k^*}^{K} P_i \mathbf{w}^H \mathbf{G}_{k^*} \mathbf{f}_{S_i R} \mathbf{f}_{S_i R}^H \mathbf{G}_{k^*}^H \mathbf{w} + \mathbf{w}^H \mathbf{G}_{k^*} \mathbf{G}_{k^*}^H \mathbf{w} \sigma^2 + \sigma^2}}{\det\left(\mathbf{I}_{2N_E} + \mathbf{H}_E \mathbf{H}_E^H \mathbf{Q}_E^{-1} \right)} \right) \right]^+ \tag{15}$$

Since the confidential signals transmitted by all the relays have been completely nulled out at Eve, the achievable secrecy rate in (12) can be rewritten as

$$R_s = \left[I(y_{k^*}; x_{k^*}) - I(\mathbf{y}_{E,1}; x_{k^*}) \right]^+, \tag{18}$$

where $I(y_{k^*}; x_{k^*})$ and $I(\mathbf{y}_{E,1}; x_{k^*})$ are given in (19) at the top of the next page.

Then the QoS based joint power allocation and CB design for the secrecy rate maximization under both the total and individual power constraints, can be formulated as the following problem:

$$\max_{\mathbf{v},\mathbf{P}} \quad R_s, \tag{20a}$$

$$s.t. \quad \gamma_k(\mathbf{v}, \mathbf{P}) \geq \gamma_k^{\min}, k \in \mathcal{K}, \tag{20b}$$

$$0 < P_k \leq P_{S_k}, \forall k \in \mathcal{K}, \quad (5) \text{ and } (6). \tag{20c}$$

The joint optimization problem (20) is difficult to solve due to the non-convexity of the objective function (20a) and constraints (20b) and (20c). In general, finding a global optimum of non-convex problem (20) is computationally expensive or even intractable. In this case, designing an efficient algorithm to compute a local maximum of the non-convex problem (20) is more meaningful in practice. In the following, with SPCA, we approximate the non-convex problem (20) into a sequence of convex problems that can be solved efficiently and obtain an efficient solution.

B. Iterative Optimization Method

Variables $P_i, i \in \mathcal{K}$ couple with $\mathbf{v}$ which is an obstacle in solving the optimization problem (20). For getting a tractable problem formulation, we introduce the following variable transformation:

$$q_k = \frac{1}{P_k}, \forall k \in \mathcal{K}, \text{ and } \mathbf{q} \triangleq \left[\frac{1}{P_1}, \ldots, \frac{1}{P_K} \right]^T. \tag{21}$$

With the variable transformation in (21), the power constraints in (5) and (6), and the SINR constraints (20b) can be rewritten respectively as

$$\sum_{k=1}^{K} \frac{\mathbf{v}^H \mathbf{U}\mathbf{F}_k \mathbf{e}_l \mathbf{e}_l^H \mathbf{F}_k^H \mathbf{U}^H \mathbf{v}}{q_k} + \mathbf{v}^H \mathbf{U}\mathbf{E}_l \mathbf{U}^H \mathbf{v} \sigma^2 \leq Q_l, \quad \forall l \in \mathcal{L}, \tag{22}$$

$$\sum_{k=1}^{K} \frac{1}{q_k} + \sum_{k=1}^{K} \frac{\mathbf{v}^H \mathbf{U}\mathbf{F}_k \mathbf{F}_k^H \mathbf{U}^H \mathbf{v}}{q_k} + \mathbf{v}^H \mathbf{U}\mathbf{U}^H \mathbf{v} \sigma^2 \leq Q_{tot}, \tag{23}$$

$$\frac{\mathbf{v}^H \mathbf{\Psi}_{k,k} \mathbf{v}}{q_k} \geq \gamma_k^{\min} \left(\sum_{i=1,i\neq k}^{K} \frac{\mathbf{v}^H \mathbf{\Psi}_{k,i} \mathbf{v}}{q_k} + \mathbf{v}^H \mathbf{\Omega}_k \mathbf{v} \sigma^2 + \sigma^2 \right), \quad \forall k \in \mathcal{K}. \tag{24}$$

It is known that, for any positive semidefinite matrix $\mathbf{A} \succeq \mathbf{0}$, the quadratic form $\mathbf{z}^H \mathbf{A} \mathbf{z}$ is convex in variable $\mathbf{z}$. Furthermore, for $g > 0$, $\frac{\mathbf{z}^H \mathbf{A} \mathbf{z}}{g}$ is the perspective of $\mathbf{z}^H \mathbf{A} \mathbf{z}$ [38, Section 3.2.6]. Since the perspective operation preserves convexity, $\frac{\mathbf{z}^H \mathbf{A} \mathbf{z}}{g}$ is jointly convex in $(\mathbf{z}, g)$ [38]. Besides, matrices $\mathbf{U}\mathbf{F}_k \mathbf{e}_l \mathbf{e}_l^H \mathbf{F}_k^H \mathbf{U}^H \succeq \mathbf{0}$, $\mathbf{U}\mathbf{F}_k \mathbf{F}_k^H \mathbf{U}^H \succeq \mathbf{0}$, and $\mathbf{\Psi}_{k,i} \succeq \mathbf{0}$, then the terms $\frac{\mathbf{v}^H \mathbf{U}\mathbf{F}_k \mathbf{e}_l \mathbf{e}_l^H \mathbf{F}_k^H \mathbf{U}^H \mathbf{v}}{q_k}$, $\frac{\mathbf{v}^H \mathbf{U}\mathbf{F}_k \mathbf{F}_k^H \mathbf{U}^H \mathbf{v}}{q_k}$, and $\frac{\mathbf{v}^H \mathbf{\Psi}_{k,i} \mathbf{v}}{q_k}$ are all jointly convex in $(\mathbf{v}, q_k)$.

We note that (24) is still a non-convex constraint, since the functions on both sides of the inequality are convex. To handle the non-convexity, we resort to SPCA which is an algorithm widely adopted for handling the non-convex problem. The basic idea of SPCA is to approximate a non-convex problem by a sequence of convex programs iteratively, where in each iteration, each non-convex constraint is replaced by an appropriate inner convex constraint. In order to apply SPCA, we should first transform the non-convex problem (20) into an appropriate form and approximate the non-convex feasible solution set by some appropriate convex subset. In the following, we adopt a two-step optimization approach to get a convex approximation of the non-convex problem (20): step 1. reformulating the problem in (20); step 2. building an appropriate convex subset that approximates the non-convex feasible solution set.

Step 1: By introducing the following variable transforma-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

$$I(y_{k^*};x_{k^*})=\frac{1}{2}\log_2\left(1+\gamma_{k^*}\left(\mathbf{v},\mathbf{P}\right)\right) \text{ and } I(\mathbf{y}_{E,1};x_{k^*})=\frac{1}{2}\log_2\left(1+P_{k^*}\mathbf{h}_{S_{k^*}E}^H\left(\sigma^2\mathbf{I}_{N_E}+\sum_{j=1,j\neq k^*}^{K}P_j\mathbf{h}_{S_jE}\mathbf{h}_{S_jE}^H\right)^{-1}\mathbf{h}_{S_{k^*}E}\right). \tag{19}$$

tion

$$\begin{aligned}
&w_B=\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*k^*}\mathbf{v}}{q_{k^*}},\\
&t_B=\frac{w_B}{\sum_{i=1,i\neq k^*}^{K}a_{k^*,i}+\beta\sigma^2+\sigma^2},\\
&a_{k^*,i}=\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*,i}\mathbf{v}}{q_i},i\in\mathcal{K}\text{ and }i\neq k^*,\\
&\beta=\mathbf{v}^H\mathbf{\Omega}_{k^*}\mathbf{v},\\
&w_E-1=\\
&\frac{\mathbf{h}_{S_{k^*}E}^H\left(\sigma^2\mathbf{I}_{N_E}+\sum_{i=1,i\neq k^*}^{K}\frac{1}{q_i}\mathbf{h}_{S_iE}\mathbf{h}_{S_iE}^H\right)^{-1}\mathbf{h}_{S_{k^*}E}}{q_{k^*}},\\
&t_E=\log_2(w_E),
\end{aligned}\tag{25}$$

we transform the problem (20) into the following equivalent problem:

$$\max_{\substack{t_B,t_E,w_B,w_E,\\ a_{k^*,i},\beta,\mathbf{v},q_k}}\ \frac{1}{2}\log_2(1+t_B)-\frac{1}{2}t_E \tag{26a}$$

$$s.t.\quad \log_2(w_E)=t_E, \tag{26b}$$

$$w_B=\sum_{i=1,i\neq k^*}^{K}t_Ba_{k^*,i}+t_B\beta\sigma^2+t_B\sigma^2, \tag{26c}$$

$$a_{k^*,i}=\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*,i}\mathbf{v}}{q_i},i\in\mathcal{K}\text{ and }i\neq k^*, \tag{26d}$$

$$\beta=\mathbf{v}^H\mathbf{\Omega}_{k^*}\mathbf{v}, \tag{26e}$$

$$\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*k^*}\mathbf{v}}{q_{k^*}}=w_B, \tag{26f}$$

$$w_E-1=\frac{1}{q_{k^*}}\mathbf{h}_{S_{k^*}E}^H\left(\sigma^2\mathbf{I}_{N_E}+\sum_{i=1,i\neq k^*}^{K}\frac{1}{q_i}\mathbf{h}_{S_iE}\mathbf{h}_{S_iE}^H\right)^{-1}\mathbf{h}_{S_{k^*}E}, \tag{26g}$$

$$(24), \tag{26h}$$

$$\frac{1}{q_k}\leq P_{S_k},k\in\mathcal{K},(22)\text{ and }(23). \tag{26i}$$

Although the objective function is concave, the optimization problem (26) is non-convex due to the non-convex equality constraints (26b)-(26g), since the functions on both sides of the equalities are not affine.

For getting a tractable problem, we should first transform the non-convex equality constraints in (26) into the equivalent inequality constraints.

$$\max_{\substack{t_B,t_E,w_B,w_E,\\ a_{k^*,i},\beta,\mathbf{v},q_k}}\ \frac{1}{2}\log_2(1+t_B)-\frac{1}{2}t_E \tag{27a}$$

$$s.t.\quad \log_2(w_E)\leq t_E, \tag{27b}$$

$$w_B\geq\sum_{i=1,i\neq k^*}^{K}t_Ba_{k^*,i}+t_B\beta\sigma^2+t_B\sigma^2, \tag{27c}$$

$$a_{k^*,i}\geq\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*,i}\mathbf{v}}{q_i},i\in\mathcal{K}\text{ and }i\neq k^*, \tag{27d}$$

$$\beta\geq\mathbf{v}^H\mathbf{\Omega}_{k^*}\mathbf{v}, \tag{27e}$$

$$\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*k^*}\mathbf{v}}{q_{k^*}}\geq w_B, \tag{27f}$$

$$w_E-1\geq\frac{1}{q_{k^*}}\mathbf{h}_{S_{k^*}E}^H\left(\sigma^2\mathbf{I}_{N_E}+\sum_{i=1,i\neq k^*}^{K}\frac{1}{q_i}\mathbf{h}_{S_iE}\mathbf{h}_{S_iE}^H\right)^{-1}\mathbf{h}_{S_{k^*}E}, \tag{27g}$$

$$(24), \tag{27h}$$

$$\frac{1}{q_k}\leq P_{S_k},k\in\mathcal{K},(22)\text{ and }(23). \tag{27i}$$

Considering the above problem (27), we would show that the optimal solution of the problem (27) is also the optimal solution of the problem (26), in the following. In particular, constraints (27b)-(27g) should be active at the optimal solution of (27).

We use the contradiction method to show that constraints (27b)-(27g) should be active, i.e., satisfy with equality at the *optimal solutions* of (27). Suppose that constraints (27b)-(27g) are not all active, i.e., *some constraints satisfy with inequality* at the optimal solution $\left(t_B^*,t_E^*,w_B^*,w_E^*,a_{k^*,i}^*,\beta^*\right)$, then we can construct a feasible point $\left(\phi_1t_B^*,\phi_2t_E^*,\phi_3w_B^*,\phi_4w_E^*,\mu_ia_{k^*,i}^*,\phi_5\beta^*\right)$, for some $\phi_1,\phi_3\geq 1$ and $0\leq\phi_2,\phi_4,\mu_i,\phi_5\leq 1$ such that constraints (27b)-(27g) are active, which is still *feasible* to the problem (27). **Note that** only the introduced variables, i.e., $(t_B,t_E,w_B,w_E,a_{k^*,i},\beta)$, are changed to make the constraints (27b)-(27g) active while $\mathbf{v}$ and q_k stay the same. For example, if only constraints (27c) and (27f) are not active, i.e., $w_B>\sum_{i=1,i\neq k^*}^{K}t_Ba_{k^*,i}+t_B\beta\sigma^2+t_B\sigma^2$ and $\frac{\mathbf{v}^H\mathbf{\Psi}_{k^*k^*}\mathbf{v}}{q_{k^*}}>w_B$, then we can construct a feasible point $\left(\phi_1t_B^*,t_E^*,\phi_3w_B^*,w_E^*,a_{k^*,i}^*,\beta^*\right)$ for some $\phi_1,\phi_3>1$ such that constraints (27c) and (27f) are active without violating other constraints. It can be seen that the new point $\left(\phi_1t_B^*,\phi_2t_E^*,\phi_3w_B^*,\phi_4w_E^*,\mu_ia_{k^*,i}^*,\phi_5\beta^*\right)$ can achieve a higher objective value than that offered by the optimal point, which leads to a contradiction. Therefore, we can conclude

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

that constraints (27b)-(27g) should be active at the optimal solutions of (27).

So far, we have already transformed the non-convex objective function of the original problem into a concave one, while the difficulties now lie in the non-convex constraints (27b)-(27h).

By introducing slack variables $u_{1,k}, u_{2,k}, \mathbf{u}_k, k \in \mathcal{K}$, constraints (27f) and (27h) can be recasted as

$$u_{1,k} = \Re\left(\mathbf{v}^H \mathbf{U}\mathbf{G}_k \mathbf{f}_{S_k R}\right), \qquad u_{2,k} = \Im\left(\mathbf{v}^H \mathbf{U}\mathbf{G}_k \mathbf{f}_{S_k R}\right),$$
$$\mathbf{u}_k \triangleq [u_{1,k}, u_{2,k}]^T, \quad k \in \mathcal{K}, \tag{28}$$

$$\frac{\mathbf{u}_{k^*}^T \mathbf{u}_{k^*}}{q_{k^*}} \geq w_B, \tag{29}$$

$$\frac{\mathbf{u}_k^T \mathbf{u}_k}{q_k} \geq \gamma_k^{\min}\left(\sum_{i=1, i\neq k}^{K} \frac{\mathbf{v}^H \mathbf{\Psi}_{k,i} \mathbf{v}}{q_i} + \mathbf{v}^H \mathbf{\Omega}_k \mathbf{v}\sigma^2 + \sigma^2\right), \quad \forall k \in \mathcal{K}. \tag{30}$$

We note that the constraints (29) and (30) are still non-convex.

Since $\frac{1}{q_i}$ is a convex function, constraint (27g) cannot be reformulated into an equivalent linear matrix inequality (LMI). The following lemma shows that the constraint (27g) has the following equivalent formulation.

Lemma 1: By exploiting Schur complement, constraint (27g) can be equivalently formulated as

$$\begin{bmatrix} \sum_{i=1, i\neq k^*}^{K} \alpha_i \mathbf{h}_{S_i E}\mathbf{h}_{S_i E}^H + \sigma^2 \mathbf{I}_{N_E} & \alpha_{k^*}\mathbf{h}_{S_{k^*}E} \\ \alpha_{k^*}\mathbf{h}_{S_{k^*}E}^H & w_E - 1 \end{bmatrix} \succeq \mathbf{0} \text{ and}$$
$$\alpha_{k^*} \geq \frac{1}{\sqrt{q_{k^*}}}, \alpha_i \leq \frac{1}{q_i}, i \in \mathcal{K}, i \neq k^*. \tag{31}$$

Proof: Setting $\alpha_i = \frac{1}{q_i}, i \in \mathcal{K}$, we can rewrite (27g) as

$$\begin{bmatrix} \sum_{i=1, i\neq k^*}^{K} \alpha_i \mathbf{h}_{S_i E}\mathbf{h}_{S_i E}^H + \sigma^2 \mathbf{I}_{N_E} & \alpha_{k^*}\mathbf{h}_{S_{k^*}E} \\ \alpha_{k^*}\mathbf{h}_{S_{k^*}E}^H & w_E - 1 \end{bmatrix} \succeq \mathbf{0} \text{ and}$$
$$\alpha_i = \frac{1}{q_i}, i \in \mathcal{K}. \tag{32}$$

Obviously, constraint (31) is equivalent to (32) if and only if the constraints $\alpha_{k^*} \geq \frac{1}{\sqrt{q_{k^*}}}, \alpha_i \leq \frac{1}{q_i}, i \neq k^*, i \in \mathcal{K}$ are all active at the optimal solutions, $\alpha_i^*, i \in \mathcal{K}$. In the following, we would adopt the contradiction method to prove that the constraints $\alpha_{k^*} \geq \frac{1}{\sqrt{q_{k^*}}}, \alpha_i \leq \frac{1}{q_i}, i \neq k^*, i \in \mathcal{K}$ should be active at the optimal solutions, $\alpha_i^*, i \in \mathcal{K}$.

If $\alpha_{k^*} \geq \frac{1}{\sqrt{q_{k^*}}}, \alpha_i \leq \frac{1}{q_i}, i \neq k^*, i \in \mathcal{K}$ are not all active at the optimal solution, $\alpha_i^*, i \in \mathcal{K}$. We can construct a feasible solution $(\nu_{k^*}\alpha_k^*, \nu_i \alpha_i^*, i \neq k^*)$ for $\nu_{k^*} \leq 1$ and $\nu_i \geq 1, i \neq k^*$ to make the constraints active. **Note that** only the introduced variables $\alpha_i, i \in \mathcal{K}$ are changed to make the constraints active. For example, if $\alpha_{k^*}^* > \frac{1}{\sqrt{q_{k^*}^*}}$, then we can construct a feasible point $(\nu_{k^*}\alpha_{k^*}^*, \alpha_i^*, i \in \mathcal{K}, , i \neq k^*)$ for some $\nu_{k^*} < 1$ such that $\nu_{k^*}\alpha_{k^*}^* = \frac{1}{\sqrt{q_{k^*}^*}}$ without violating other constraints. It can be seen that the new point $(\nu_{k^*}\alpha_k^*, \nu_i\alpha_i^*, i \neq k^*)$ would result in a smaller w_E. This can be explained by the fact that w_E can be decreased further without violating the constraint (31). Therefore, a larger objective value than that offered by the optimal point can be achieved, which leads to a contradiction. Therefore, $\alpha_{k^*} \geq \frac{1}{\sqrt{q_{k^*}}}, \alpha_i \leq \frac{1}{q_i}, i \in \mathcal{K}$ should be active at the optimal solution and the equivalence can be proved. ■

With (28)-(31), the problem (27) is transformed into the following equivalent problem

$$\max_{\substack{t_B, t_E, w_B, w_E, u_{1,i}, u_{2,i} \\ a_{k^*,i}, \alpha_i, \beta, \mathbf{v}, \mathbf{u}_i, q_i}} \frac{1}{2}\log_2(1 + t_B) - \frac{1}{2}t_E, \tag{33a}$$

$$s.t.\ (27b) - (27e),\ (28)\text{-}(30),\ (27i) \text{ and } (31). \tag{33b}$$

Step 2: The problem (33) is still non-convex, since constraints (27b), (27c), (29), (30), and, (31) are all non-convex. In the following, for adopting SPCA to handle the problem (33), we first approximate the non-convex feasible set by an appropriate inner convex feasible set.

In particular, assuming that $w_E(l-1)$, $a_{k^*,i}(l-1)$, $t_B(l-1)$, $\beta(l-1)$, $\mathbf{u}_i(l-1)$, and $q_i(l-1)$ are the optimal solutions of the convex approximation program at the $(l-1)$th iteration, we approximate the non-convex terms in (27b), (29), (30), and (31) by their first-order Taylor approximations around the optimal solutions at the $(l-1)$th iteration, which are given as follows

$$\Gamma(w_E; w_E(l-1)) \triangleq \log_2(w_E(l-1)) + \frac{w_E - w_E(l-1)}{w_E(l-1)\ln(2)}, \tag{34}$$

$$\Xi_i\left(\mathbf{s}_i; \mathbf{s}_i(l-1)\right) \triangleq \frac{\mathbf{u}_i(l-1)^T\mathbf{u}_i(l-1)}{q_i(l-1)} - \frac{\mathbf{u}_i(l-1)^T\mathbf{u}_i(l-1)}{q_i^2(l-1)}$$
$$(q_i - q_i(l-1)) + \frac{2\mathbf{u}_i^T}{q_i(l-1)}\left(\mathbf{u}_i - \mathbf{u}_i(l-1)\right), \tag{35}$$

$$\Upsilon_j\left(q_j; q_j(l-1)\right) \triangleq \frac{1}{q_j(l-1)} - \frac{1}{q_j^2(l-1)}\left(q_j - q_j(l-1)\right), \tag{36}$$

where $\mathbf{s}_i \triangleq [q_i; \mathbf{u}_i]$.

The non-convex term in the constraint (27c) is approximated by the following function

$$\sum_{j=1, j\neq k^*}^{K} H_j(t_B, a_{k^*,j}; \theta_j(l)) + \Lambda(t_B, \beta; \lambda(l))\sigma^2 + t_B\sigma^2, \tag{37}$$

where $H_j(t_B, a_{k^*,j}; \theta_j(l)) \triangleq \frac{\theta_j(l)}{2}t_B^2 + \frac{1}{2\theta_j(l)}a_{k^*,j}^2$, $\Lambda(t_B, \beta; \lambda(l)) \triangleq \frac{\lambda(l)}{2}t_B^2 + \frac{1}{2\lambda(l)}\beta^2$, and $\theta_j(l) = \frac{a_{k^*,j}(l-1)}{t_B(l-1)}$, $\lambda(l) = \frac{\beta(l-1)}{t_B(l-1)}$.

With the above approximations, the proposed iterative algorithm for the joint power allocation and beamformer design is summarized in Algorithm 1, where the convex approximation program (38) is solved at the lth iteration. As shown in the proof of Lemma 2, the feasible set defined by (38b)-(38j) is a subset of the original feasible set defined by (33b). Consequently, if the initial points $w_E(0), t_B(0), a_{k^*,j}(0)$, $\beta(0), \mathbf{u}_i(0), q_i(0)$ are feasible for the problem (38), the solutions generated by solving the problem in (38) iteratively always belong to the original feasible set defined by (33b). The procedure is carried out iteratively until convergence or until the maximum number of allowable iterations is reached. In Algorithm 1, the feasible initial points are assumed to be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

Algorithm 1 Iterative joint power allocation and beamformer design algorithm.

Set the tolerance of accuracy ϵ and the maximum number of iterations $N^{\max}$. Initialize the algorithm with feasible points $w_E(0), t_B(0), a_{k^*,j}(0), \beta(0), \mathbf{u}_i(0), q_i(0)$ and the corresponding parameters $\theta_j(1), \lambda(1)$ can be calculated as $\theta_j(1) = \frac{a_{k^*,j}(0)}{t_B(0)}$, $\lambda(1) = \frac{\beta(0)}{t_B(0)}$. Set the iteration number $l = 1$.

while The difference of the objective function in successive iterations is larger than ϵ and the maximum number of iterations is not reached, i.e., $l \leq N^{\max}$ **do**

Solve the optimization problem (38)

Set $\theta_j(l+1) = \frac{a_{k^*,j}(l)}{t_B(l)}, \lambda(l+1) = \frac{\beta(l)}{t_B(l)}$, $l = l+1$,

end while

Output: $\mathbf{v}, \frac{1}{q_j}$.

available and in Section III-C, an efficient iterative algorithm would be provided to find the feasible initial points.

$$\max_{\substack{t_B,t_E,w_B,w_E,\mathbf{u}_i,\\ u_{1,i},u_{2,i},a_{k^*,j},\alpha_j,\beta,\mathbf{v},q_i}} \frac{1}{2}\log_2(1+t_B) - \frac{1}{2}t_E \tag{38a}$$

$$s.t. \quad \Gamma(w_E; w_E(l-1)) \leq t_E, \tag{38b}$$

$$w_B \geq \sum_{j=1,j\neq k^*}^{K} H_j(t_B, a_{k^*,j}; \theta_j(l)) + \Lambda(t_B, \beta; \lambda(l))\sigma^2 + t_B\sigma^2, \tag{38c}$$

$$a_{k^*,j} \geq \frac{\mathbf{v}^H \mathbf{\Psi}_{k^*,j}\mathbf{v}}{q_j}, j \in \mathcal{K} \text{ and } j \neq k^*, \tag{38d}$$

$$\beta \geq \mathbf{v}^H \mathbf{\Omega}_{k^*}\mathbf{v}, \tag{38e}$$

$$(28), \tag{38f}$$

$$\Xi_{k^*}(\mathbf{s}_{k^*}; \mathbf{s}_{k^*}(l-1)) \geq w_B, \tag{38g}$$

$$\Xi_i(\mathbf{s}_i; \mathbf{s}_i(l-1)) \geq \gamma_i^{\min}\left(\sum_{j=1,j\neq i}^{K} \frac{\mathbf{v}^H \mathbf{\Psi}_{i,j}\mathbf{v}}{q_j} + \mathbf{v}^H \mathbf{\Omega}_i \mathbf{v}\sigma^2 + \sigma^2\right), i \in \mathcal{K} \tag{38h}$$

$$\begin{bmatrix} \sum_{j=1,j\neq k^*}^{K} \alpha_j \mathbf{h}_{S_j E}\mathbf{h}_{S_j E}^H + \sigma^2 \mathbf{I}_{N_E} & \alpha_{k^*}\mathbf{h}_{S_{k^*}E} \\ \alpha_{k^*}\mathbf{h}_{S_{k^*}E}^H & w_E - 1 \end{bmatrix} \succeq \mathbf{0}, \tag{38i}$$

$$\alpha_{k^*} \geq \frac{1}{\sqrt{q_{k^*}}}, \quad \alpha_j \leq \Upsilon_j(q_j; q_j(l-1)), j \in \mathcal{K}, j \neq k^*, \tag{38j}$$

$$(27i), \tag{38j}$$

The following lemma shows that the solutions obtained by Algorithm 1 is the feasible solutions of the non-convex problem (33).

Lemma 2: The solutions obtained by Algorithm 1 lie in the feasible set of the non-convex problem (33).

Proof: The proof is given in Appendix A. ∎

In what follows, a theorem regarding the convergence of Algorithm 1 is given.

Theorem 1: The optimal value of the objective function in the problem (38) is non-decreasing as the iteration number l increases.

Proof: The proof is given in Appendix B. ∎

As indicated by Theorem 1, the optimal objective value of the problem (38) is non-decreasing as the iteration number l increases, hence ensuring monotonicity. Further, owing to the power constraints the maximal achievable secrecy rate is bounded above. Therefore, the proposed iterative procedure is guaranteed to converge.

C. The Proposed Feasible Initial Points Search Algorithm

The main advantage of Algorithm 1 is that once the initial point is feasible to the problem in (33), all the solutions generated iteratively by Algorithm 1 remain within the feasible set of the problem (33). However, if Algorithm 1 is initialized with the random points, it may fail at the first iteration due to the infeasibility of the problem (38). Hence, the feasible initial point is of great importance. The problem (33) is non-convex and the task of calculating a feasible solution for the problem (33) can be shown to be NP-hard [32]. Therefore, a low-complexity algorithm for calculating the initial points of the problem (33) is very important for implementing Algorithm 1 to optimize the beamformer and power allocation jointly. Inspired by [28], [30], we propose an efficient iterative algorithm for calculating the initial points of the problem (33).

Let us introduce a real-valued parameter $z > 0$, which can be regarded as a measure of how far the corresponding constraints in (38) is from being satisfied, i.e., *an infeasibility indicator*. We formulate the feasibility problem as follows:

$$\min_{\substack{z,t_B,t_E,w_B,w_E,u_{1,i},u_{2,i}\\ \mathbf{u}_i,a_{k^*,j},\alpha_j,\mathbf{u}_i,\beta,\mathbf{v},q_i}} z \tag{39a}$$

$$s.t. \quad \Gamma(w_E; w_E(l)) - t_E \leq z, \tag{39b}$$

$$\sum_{j=1,j\neq k^*}^{K} H_j(t_B, a_{k^*,j}; \theta_j(l)) + \Lambda(t_B, \beta; \lambda(l))\sigma^2 + t_B\sigma^2 - w_B \leq z, \tag{39c}$$

$$\frac{\mathbf{v}^H \mathbf{\Psi}_{k^*,j}\mathbf{v}}{q_j} - a_{k^*,j} \leq z, j \in \mathcal{K} \text{ and } j \neq k^*, \tag{39d}$$

$$\mathbf{v}^H \mathbf{\Omega}_{k^*}\mathbf{v} - \beta \leq z, \tag{39e}$$

$$(28), \tag{39f}$$

$$w_B - \Xi_{k^*}(\mathbf{s}_{k^*}; \mathbf{s}_{k^*}(l-1)) \leq z, \tag{39g}$$

$$\gamma_i^{\min}\left(\sum_{j=1,j\neq i}^{K} \frac{\mathbf{v}^H \mathbf{\Psi}_{i,j}\mathbf{v}}{q_j} + \mathbf{v}^H \mathbf{\Omega}_i \mathbf{v}\sigma^2 + \sigma^2\right) - \Xi_i(\mathbf{s}_i; \mathbf{s}_i(l-1)) \leq z, i \in \mathcal{K}, \tag{39h}$$

$$\begin{bmatrix} \sum_{j=1,j\neq k^*}^{K} \alpha_j \mathbf{h}_{S_j E}\mathbf{h}_{S_j E}^H + \sigma^2 \mathbf{I}_{N_E} & \alpha_{k^*}\mathbf{h}_{S_{k^*}E} \\ \alpha_{k^*}\mathbf{h}_{S_{k^*}E}^H & w_E - 1 \end{bmatrix} \succeq \mathbf{0}, \tag{39i}$$

$$\frac{1}{\sqrt{q_{k^*}}} - \alpha_{k^*} \leq z, \alpha_j - \Upsilon_j(q_j; q_j(l)) \leq z, j \in \mathcal{K}, j \neq k^*, \tag{39j}$$

$$(27i). \tag{39k}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

Algorithm 2 Feasible initial points searching algorithm.

Set the tolerance of accuracy $0 < \varrho \ll 1$ and the maximum number of iterations $N^{\max}$. Initialize the algorithm with a random point $w_E(0), t_B(0), a_{k^*,j}(0), \beta(0), \mathbf{u}_i(0), q_i(0)$ and the corresponding parameters $\theta_j(1), \lambda(1)$ can be calculated as $\theta_j(1) = \frac{a_{k^*,j}(0)}{t_B(0)}$, $\lambda(1) = \frac{\beta(0)}{t_B(0)}$. Set the iteration number $l = 1$.

while $z > \varrho$ and the maximum number of iterations is not reached, i.e., $l \leq N^{\max}$ **do**

Solve the problem (39)

Set $\theta_j(l+1) = \frac{a_{k^*,j}(l)}{t_B(l)}, \lambda(l+1) = \frac{\beta(l)}{t_B(l)}$, $l = l + 1$,

end while

Output: $w_E, t_B(l), a_{k^*,j}, \beta, \mathbf{u}_i, q_i$.

The proposed feasible initial point searching algorithm, summarized in Algorithm 2, is based on a similar iterative approximation method adopted in Algorithm 1. Specifically, the non-convex constraints in (33) are approximated by the appropriate convex constraints at each iteration. Since Algorithm 2 is based on a similar iterative approximation method adopted in Algorithm 1, we have the following proposition about Algorithm 2.

Proposition 1: The optimal solution of the problem (39) at the $(l-1)$th iteration is a feasible solution of the problem (39) at the lth iteration. Therefore, the optimal value of the objective function in the problem (39) is non-increasing as the iteration number l increases. Algorithm 2 is guaranteed to converge.

Proof: The proof is similar to the proofs of Lemma 2 and Theorem 1, which is omitted for brevity. ■

Different from Algorithm 1, Algorithm 2 starts with random initial points and if at the lth iteration, the current objective value z is zero, the algorithm stops, otherwise, the algorithm continues until z is zero or the maximum number of the allowable iterations is reached. If no feasible point is obtained for some system parameters, e.g., QoS constraints and power constraints, some system parameters should be relaxed to get a feasible solution. We note that if Algorithm 2 fails to provide a feasible initial point, it does not imply that this problem is infeasible as Algorithm 2 is an approximate algorithm which operates at the convex subset of the original nonconvex feasible solution set of the problem (33).

D. Complexity Analysis

In this subsection, we study the computational complexity of the proposed Algorithm by revealing the joint computational complexity of Algorithm 1 and 2. Comparing the problem (38) with (39), we can find that they have a similar structure and the computational complexities for solving the problem (38) and (39) are almost the same. The optimization problem (38) is a semidefinite programming (SDP), and using Schur complements, all of the constraints in (38) can be transformed into LMIs. Although it is not a standard SDP problem [38], when the interior-point method is employed to solve the problem (38), as shown in [41], the worst-case complexity can be calculated by $\mathcal{O}\left(n^2\left(\sum_i n_i^2\right)\sqrt{\sum_i n_i}\right)$, where n is the number of optimization variables and n_i is the dimension of the ith semidefinite cone. Therefore, when the interior-point method is employed to solve the problem (38), the worst-case computational complexity can be calculated by

$$\mathcal{O}\Big((L-N_E)^2\left((K^2+K)(L-N_E+1)^2+(N_E+1)^2\right)\sqrt{(K^2+K)(L-N_E+1)+(N_E+1)}\Big). \quad (40)$$

Therefore, the sum of the computational complexity of the proposed algorithm can be calculated by $(T_1 + T_2)$ times of the complexity of solving the problem (38) and (39) at each iteration, where T_1 and T_2 are the required numbers of iterations for Algorithm 1 and 2.

IV. Simulation Results

In simulations, we assume that the channels among each pair of nodes are *i.i.d.* complex Gaussian variable with zero mean and unit variance. The Gaussian noise power σ^2 is normalized to be 0 dBm. The maximum number of iterations $N^{\max}$ in Algorithm 1 and 2 is 18. In particular, we set $Q_{tot} = P_M$, $P_{S_k} = \frac{1.5P_M}{K}, Q_l = \frac{2P_M}{L}$, and $\gamma_l^{\min} = \gamma^{\min}, \forall k \in \mathcal{K}, l \in \mathcal{L}$. The following simulation results are provided to illustrate the performance of the proposed algorithm, and all of the simulation results were averaged over 1000 independent channel realizations.

In Fig. 2 and Fig. 3, the average convergence behavior of our proposed algorithms is illustrated for the MUP2P relay network with $K = 3, N_E = 3$, and different L. In particular, in Fig. 2, we set $\varrho = 0.001$ for the infeasibility indicator z in (39a) and plot its value versus the iteration number. From Fig. 2, we can find that the average convergence of Algorithm 2 is very fast and Algorithm 2 converges to an efficient solution in less than 4 iterations. Furthermore, the convergence rate increases with increasing L. In Fig. 3, setting $\epsilon = 0.001$, the average convergence speed of Algorithm 1 is illustrated. Simulation results show that Algorithm 1 converges within about 15 iterations for any feasible points. Besides, there is no particular relationship between the convergence behavior of Algorithm 1 and the number of the relay nodes, which comfirms the practicality of our proposed algorithm.

In Fig. 4, the average secrecy rate achieved by the proposed algorithm is depicted versus P_M for different L. To show the secure performance gains achieved by the proposed algorithm, for $L = 10, K = 3, N_E = 3$, "Interference Cancellation" is provided for the performance comparison. Specifically, assuming that the equal power allocation is adopted at multiple sources, i.e, $P_1 = \ldots, = P_K = P$, we make the relay beamforming $\mathbf{w}^*$ lie in the null space of $\mathbf{\Phi}$ to eliminate the co-channel interference in (7) and the confidential information leakage in Phase II, and $\mathbf{\Phi}$ is given by

$$\mathbf{\Phi} \triangleq \left[\mathbf{\Pi}_{D_1}, \ldots, \mathbf{\Pi}_{D_K}, \left(\mathbf{C}_E\mathbf{F}_{k^*}\right)^T\right]^T,$$
$$\mathbf{\Pi}_{D_k} \triangleq \left[\mathbf{G}_k\mathbf{f}_{S_1R}, \ldots, \mathbf{G}_k\mathbf{f}_{S_{k-1}R}, \mathbf{G}_k\mathbf{f}_{S_{k+1}R}, \ldots, \mathbf{G}_k\mathbf{f}_{S_KR}\right]. \quad (41)$$

When $L > K(K-1) + N_E$, the null space of $\mathbf{\Phi}$ exists and can be obtained. In particular, for $L = 10, K = 3, N_E = 3$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

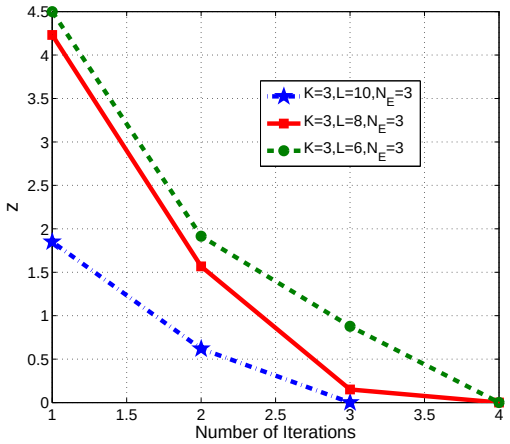

Fig. 2. The objective value in (39a) versus the number of iterations for $K = 3, N_E = 3, L = 10, 8, 6, P_M = 20$ dBm, $\gamma^{\min} = 1$, and $\varrho = 0.001$.

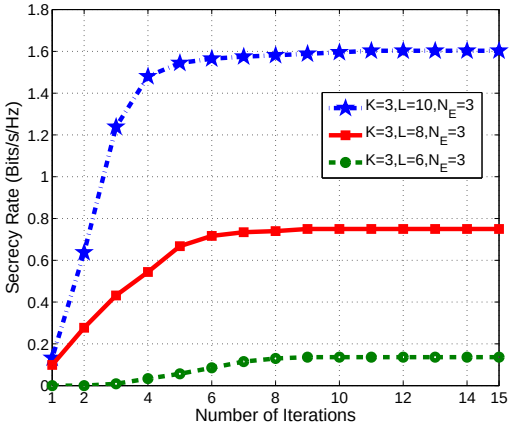

Fig. 3. Secrecy rate achieved by the proposed algorithm versus the number of iterations for $K = 3, N_E = 3, L = 10, 8, 6, P_M = 20$ dBm, $\gamma^{\min} = 1$, $\epsilon = 0.001$, and $\varrho = 0.001$.

the null space of $\mathbf{\Phi}$ is a $L \times 1$ vector $\mathbf{t}$ such that $\mathbf{\Phi t} = \mathbf{0}$. In "Interference Cancellation", $\mathbf{t}$ is adopted as the relay beamforming. Then the received SNR at the kth destination, i.e., $\hat{\gamma}_k$ can be calculated by

$$\hat{\gamma}_k = P\mathbf{t}^H \mathbf{G}_k \mathbf{f}_{s_k R} \mathbf{f}_{s_k R}^H \mathbf{G}_k \mathbf{t}, \tag{42}$$

and the rate achieved by the eavesdropper can be calculated by

$$I(\mathbf{y}_{E,1}; x_{k^*}) = \frac{1}{2}\log_2\Bigg(1 + P\mathbf{h}_{S_{k^*}E}^H \left(\sigma^2 \mathbf{I}_{N_E} + \sum_{j=1, j\neq k^*}^{K} P\mathbf{h}_{S_j E}\mathbf{h}_{S_j E}^H\right)^{-1} \mathbf{h}_{S_{k^*}E}\Bigg). \tag{43}$$

In " Interference Cancellation", we assume that the full power transmission is adopted and the transmit power of the sources, P can be adjusted to satisfy the individual and total power constraint. From Fig. 4, we can find that comparing with our proposed algorithm, the performance degradation of "Interference Cancellation" is severe. This is due to the fact that most of

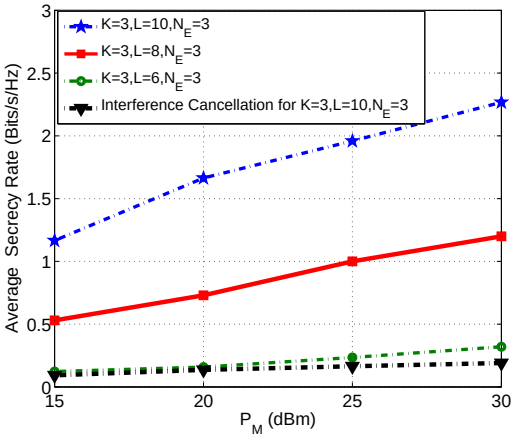

Fig. 4. Average secrecy rate achieved by the proposed Algorithm and "Interference Cancellation" versus P_M for $K = 3, N_E = 3, L = 10, 8, 6$ $\gamma^{\min} = 1$, $\epsilon = 0.001$, and $\varrho = 0.001$.

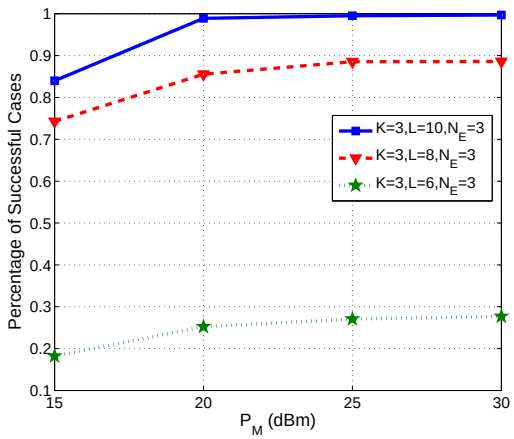

Fig. 5. Percentage of successful cases versus P_M for $K = 3, N_E = 3$, $L = 10, 8, 6$, $\gamma^{\min} = 1$, and $\varrho = 0.001$.

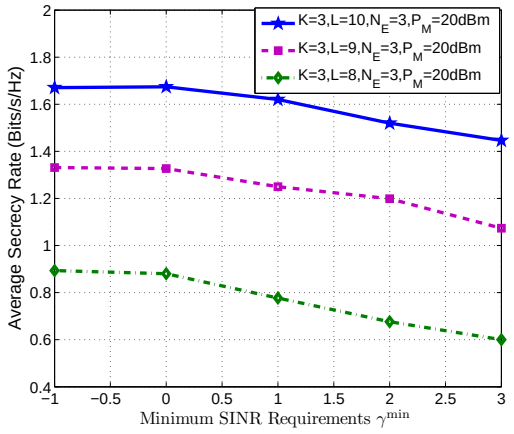

Fig. 6. Average secrecy rate achieved by the proposed algorithm versus the minimum SINR requirement $\gamma^{\min}$ for $K = 3, N_E = 3, L = 10, 9, 8$, $P_M = 20$ dBm, $\epsilon = 0.001$, and $\varrho = 0.001$.

the spatial degrees-of-freedom (DOF) is used for eliminating the co-channel interference and which loses the transmit diversity. Furthermore, for the equal power allocation, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

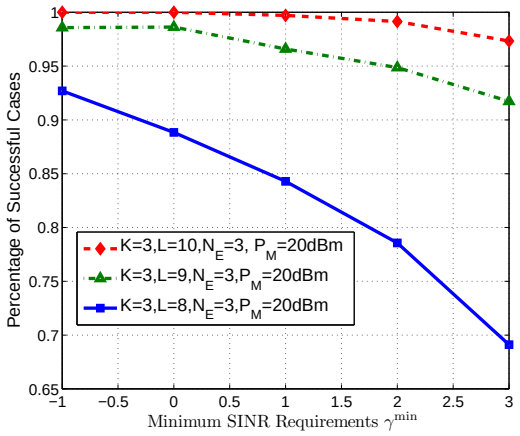

Fig. 7. Percentage of successful cases versus the minimum SINR requirement $\gamma^{\min}$ for $K = 3, N_E = 3$, $L = 10, 9, 8$, $P_M = 20$ dBm, and $\varrho = 0.001$.

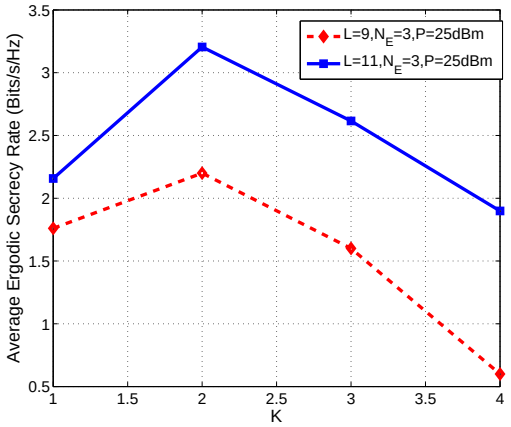

Fig. 8. Average secrecy rate achieved by the proposed algorithm versus the number of users for $L = 9, 11, N_E = 3, \gamma^{\min} = 1, P = 25$ dBm, $\epsilon = 0.001$, and $\varrho = 0.001$.

transmit power at the secure user and unclassified users cannot be allocated efficiently for maximizing the achievable secrecy rate, which also leads to the performance degradation. However, considering our proposed secure transmission scheme, with the cooperative beamforming, the weights multiplied at relay nodes are optimized jointly for maximizing the confidential signal strength received at the desired destination. Therefore, the reception capability of the desired destination is improved. Furthermore, for satisfying the QoS constraint at each destination, the transmit power of each user should be much larger than the noise power. Therefore, in practice, the co-channel interference from multiple users is the dominated interference term received at the eavesdropper and destired destination. Exploiting the dominated co-channel interference term, our proposed joint beamforming and power allocation algorithm optimizes the power allocation among multiple users, and the beamformer jointly for increasing the received interference at the eavesdropper and decreasing the co-channel interference power at the desired destination, which improves the quality of secrecy communication of the desired destination. Therefore, our proposed secure transmission scheme can achieve such a good secrecy performance in the simulation.

As P_M increases, more power can be coordinated to interfere with Eve and send the desired signals, therefore, the average secrecy rate increases with P_M. Furthermore, with increasing L, more DOF can be utilized to increase the transmit diversity and improve the achievable secrecy rate. Therefore, compared with $L = 6, 8$, the proposed scheme achieves the best performance for $L = 10$.

In Fig. 5, we depict the percentage of successful cases achieved by Algorithm 2 versus P_M for different L. Simulation results show that with increasing L and P_M, the percentage of successful cases is increasing. The simulation results are intuitive, since with the increasing available resources, i.e., transmit power and spatial DOF, the feasibility of the non-convex problem would be improved.

In Fig. 6, the average secrecy rate achieved by the proposed algorithm is depicted versus the minimum SINR requirement $\gamma^{\min}$ for different L. Simulation results show that the achievable secrecy rate decreases with increasing $\gamma^{\min}$. This could be explained by the fact that, as $\gamma^{\min}$ rises, more power is allocated to maintain the minimum achieved SINR for each destination. Fig. 7 shows the percentage of successful cases achieved by Algorithm 2 with increasing $\gamma^{\min}$ for different L. Fig. 7 indicates that the feasibility of Algorithm 2 can be improved substantially by increasing L.

In Fig. 8, the average secrecy rate achieved by the proposed algorithm is depicted versus the number of users, K, for different L. Simulation results show that with increasing K, the achievable secrecy rate first increases and then decreases. This can be explained by the fact that although with increasing K, more jamming signals from the unclassified users can be coordinated to interfere with the eavesdropper, the interference at each destination increases due to the QoS constraint. Furthermore, for satisfying the QoS constraint at each user, each user would consume some power. Therefore, with the increasing K, the available transmit power for each user decreases due to the total power constraint. Then the achievable secrecy rate would decrease with the decreasing power budget of the secure user.

V. Conclusion

In this paper, we investigate the security issue of the AF MUP2P relay networks, where a secure user transmits the confidential information in the presence of a multi-antenna eavesdropper, while the other unclassified users transmit unclassified messages. We jointly design the transmit power of the source and relay beamformer for maximizing the achievable secrecy rate under the minimum received SINR requirement at each destination. Although the resulting problem is non-convex, we propose a low computational complexity iterative algorithm to obtain an efficient solution. Specifically, through adopting SPCA, the non-convex problem is transformed into a sequence of convex approximation problems with appropriate inner convex approximation constraints. We also propose a feasible initial points searching algorithm which, in conjunction with Algorithm 1, helps to solve the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

joint resource allocation design. We show that the proposed iterative algorithm is assured to converge and numerical results confirm the effectiveness of the proposed algorithms.

APPENDIX A
PROOF OF LEMMA 2

To show that the convergent solutions obtained by Algorithm 1 lie in the feasible set of the non-convex problem (33), we should prove that the feasible set of the approximation program (38) is the *inner convex approximations* of the original non-convex problem (33). In other words, the optimal solution of the approximate problem (38) definitely belongs to the feasible set of the original non-convex optimization problem (33).

Since the function $\log_2(w_E)$ is concave, $\frac{1}{q_j}$ is convex, and the function $\frac{\mathbf{u}_i^T\mathbf{u}_i}{q_i}$ is jointly convex in the variables $(\mathbf{u}_i, q_i)$, according to the first conditions of the convex function [38], we have that $\log_2(w_E) \leq \Gamma(w_E; w_E(l-1))$, $\Xi_i\left(\mathbf{s}_i; \mathbf{s}_i(l-1)\right) \leq \frac{\mathbf{u}_i^T\mathbf{u}_i}{q_i}$ and $\Upsilon_j\left(q_j, q_j(l-1)\right) \leq \frac{1}{q_j}$. Therefore, replacing the non-convex terms in (27b), (29), (30), and (31) by their first-order Taylor approximations, will result in an inner convex approximation. Furthermore, since the non-convex terms in (27c) have the similar structure as $t_B\beta$, in the following, we only prove that replacing $t_B\beta$ by $\Lambda\left(t_B, \beta; \lambda(l)\right)$ will result in an inner convex approximation. Then, the proof that $\sum_{j=1, j\neq k^*}^{K} t_B a_{k^*,j}$ can be approximated by $\sum_{j=1, j\neq k^*}^{K} H_j(t_B, a_{k^*,j}; \theta_j(l))$, would be achieved with a similar procedure, which is omitted for brevity. Since $\Lambda\left(t_B, \beta; \lambda(l)\right) - t_B\beta = \frac{1}{2}\left(\sqrt{\lambda(l)}t_B - \frac{1}{\sqrt{\lambda(l)}}\beta\right)^2 \geq 0$, $\Lambda\left(t_B, \beta; \lambda(l)\right) \geq t_B\beta$. Then, we can conclude that replacing $t_B\beta$ by $\Lambda\left(t_B, \beta; \lambda(l)\right)$ will result in an inner convex approximation. ■

APPENDIX B
PROOF OF THEOREM 1

In the following, we first show that the optimal solution of the problem (38) at the $(l-1)$th iteration is also a feasible solution of the problem (38) at the lth iteration.

For showing the optimal solution at the $(l-1)$th iteration is a feasible solution for the optimization problem at the lth iteration, we should prove that the optimal solution at the $(l-1)$th iteration satisfies all the constraints of the optimization problem at the lth iteration. Now, we show that the optimal solution at the $(l-1)$th iteration satisfies the constraint (38b) of the problem at the lth iteration, i.e., $\Gamma(w_E(l-1); w_E(l-1)) \leq t_E(l-1)$.

Since $w_E(l-1)$ is the optimal solution at the $(l-1)$th iteration, we have

$$\Gamma(w_E(l-1); w_E(l-2)) \leq t_E(l-1). \tag{44}$$

Since $\log_2(w_E)$ is a concave function of w_E, and $\Gamma(w_E; w_E(l-2))$ is the first Taylor expansion around the optimal solution $w_E(l-2)$ at the $(l-2)$iteration, according to the first-order conditions of the concave function, we have

$$\log_2(w_E(l-1)) \leq \Gamma(w_E(l-1); w_E(l-2)). \tag{45}$$

Then combining (44) and (45), we have

$$\log_2(w_E(l-1)) \leq t_E(l-1). \tag{46}$$

As we know $\Gamma(w_E(l-1); w_E(l-1)) = \log_2(w_E(l-1))$, we can conclude that $\Gamma(w_E(l-1); w_E(l-1)) \leq t_E(l-1)$. Therefore, the optimal solutions at the $(l-1)$th iteration satisfy constraint (38b).

With a similar procedure, we can prove that the optimal solution at the $(l-1)$th iteration satisfies other constraints of the problem at the lth iteration, which is omitted for brevity. Therefore, we can conclude that the optimal solution at the $(l-1)$th iteration is a feasible solution for the optimization problem at the lth iteration. Since the optimal solution at the $(l-1)$th iteration is also a feasible solution of the problem (38) at the lth iteration, the optimal value of the problem (38) at the lth iteration should be no less than the one at the $(l-1)$th iteration. Therefore, we can conclude that the optimal value of the objective function in the problem (38) is non-decreasing as the iteration number l increases. ■

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355-1387, 1975.

[2] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory,* Seattle,WA, Jul. 2006.

[3] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jul. 2007.

[4] S. L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 26, no. 4, pp. 451-456, Jul. 1978.

[5] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay network," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528-3540, Oct. 2011.

[6] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel", *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[7] A. Khisti and G.Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[8] S. A. A. Fakoorian and A. Lee Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620-2631, May 2013.

[9] M. F. Hanif, L.-N. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Trans. Signal Process.*, vol. 62, no. 14, pp. 3536-3551, Jul. 2014.

[10] G. Zheng, P. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852-863, Feb. 2012.

[11] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Infor. Forensics and Sec.,* vol. 9, no. 11, pp. 1814-1827, Nov. 2014

[12] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches,"*IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29-40, Sep. 2013.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[14] J. Li, A. P. Petropulu, and S.Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[15] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: low complexity design," *IEEE Trans. Veh. Technol.*, pre-print 2015, available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6847741

[16] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, pre-print, 2015, available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6955810

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

[17] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35-39, Jan. 2013.

[18] H.-M. Wang, Q. Yin, and X-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3632, Jul. 2012.

[19] Y. Yang, C. Sun, H. Zhao, H. Long, and W. Wang, "Algorithms for secrecy guarantee with null space beamforming in two-way relay networks," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 2111-2126, Apr. 2014.

[20] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. on Wireless Commun*, vol. 6, no. 9, pp. 3450-3460, Sep. 2007.

[21] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*,vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[22] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[23] H.-M. Wang, M. Luo, Q. Yin, and X-G. Xia, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdroppers CSI," *IEEE Signal Process. Lett,* vol. 20, no. 1, pp. 39-42, Jan. 2013.

[24] 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 Trans. on Inf. Forensics and Security,* vol. 8, no. 12, pp. 2007-2020, Dec. 2013.

[25] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. on Wireless Commun.*, pre-print, 2015, available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6891384

[26] C. Wang, H.-M. Wang, X.-G. Xia, and Chaowen Liu "Uncoordinated Jammer Selection for Securing SIMOME Wiretap Channels: A Stochastic Geometry Approach," *IEEE Trans. on Wireless Commun.*, pre-print, 2015, available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7005544

[27] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379-389, Feb. 2007.

[28] Y. Cheng and M. Pesavento, "Joint optimization of source power allocation and distributed relay beamforming in multiuser peer-to-peer relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 2962-2973, Jun. 2012.

[29] S. Fazeli-Dehkordy, S. Shahbazpanahi, and S. Gazor, "Multiple peer-to-peer communications using a network of relays," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3053-3062, Aug. 2009.

[30] N. Bornhorst, M. Pesavento, and A. B. Gershman, "Distributed beamforming for multi-group multicasting relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 221-232, Jan. 2012.

[31] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[32] C. D'Ambrosio, A. Frangioni, L. Liberti, and A. Lodi, Mathematical Programming, "A storm of feasibility pumps for nonconvex MINLP," 2011 [Online]. Available: http://www.di.unipi.it/∼frangio/papers/fpminlp.pdf

[33] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 503-506, Oct. 2013.

[34] T. Kwon, V. W.S. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012.

[35] Q. Li and W.-K Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704-2717, May. 2013.

[36] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP)*, 2012, Kyoto, Japan, Mar. 2012.

[37] H. Ochiai, P. Mitran, H. V. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4110-4124, Nov. 2005

[38] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[39] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Operat. Res.*, vol. 26, pp. 681-683, 1978.

[40] A. Beck, A. Ben-Tal, and L. Tetruashvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *J. Global Optim.*, vol. 47, no. 1, pp. 29-51, May. 2010.

[41] J. F. Sturm, "Implementation of interior point methods for mixed semidefinite and second order cone optimization problems," *Optim. Meth. Softw.,* vol. 17, no. 6, pp. 1105-1154, 2002.

Chao Wang received the B.S. degree in Telecommunication Engineering in 2008, and the M.S. degree in Information and Communication Engineering in 2013 from Xi'an Jiaotong University, respectively. He is currently working towards the Ph.D. degree in Information and Communication Engineering, Xi'an Jiaotong University. His research interests include cooperative communications, MIMO systems, stochastic geometry, and physical-layer security of wireless communications.

Chao Wang received a Best Paper Award of IEEE/CIC International Conference on Communications in China, 2014.

Hui-Ming Wang (S'07, M'10) received the B.S. and Ph.D. degrees, both in Electrical Engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and 2010, respectively. He is currently a Full Professor with the Department of Information and Communications Engineering, Xi'an Jiaotong University, and also with the Ministry of Education Key Lab for Intelligent Networks and Network Security, China. From 2007 to 2008, and 2009 to 2010, he was a Visiting Scholar at the Department of Electrical and Computer Engineering, University of Delaware, USA. His research interests include cooperative communication systems, physical-layer security of wireless communications, MIMO and space-timing coding.

Dr. Wang received the National Excellent Doctoral Dissertation Award in China in 2012, a Best Paper Award of International Conference on Wireless Communications and Signal Processing, 2011, and a Best Paper Award of IEEE/CIC International Conference on Communications in China, 2014.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2403367, IEEE Transactions on Wireless Communications

Derrick Wing Kwan Ng (S'06-M'12) received the bachelor degree with first class honors and the Master of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively. He received his Ph.D. degree from the University of British Columbia (UBC) in 2012. In the summer of 2011 and spring of 2012, he was a visiting scholar at the Centre Tecnològic de Telecomunicacions de Catalunya - Hong Kong (CTTC-HK). He is now working as a postdoctoral fellow in the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg (FAU), Germany. His research interests include cross-layer optimization for wireless communication systems, resource allocation in OFDMA wireless systems, and communication theory.

Dr. Ng received the Best Paper Awards at the IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008. He was awarded the IEEE Student Travel Grants for attending the IEEE WCNC 2010, the IEEE International Conference on Communications (ICC) 2011, and the IEEE Globecom 2011. He was also the recipient of the 2009 Four Year Doctoral Fellowship from the UBC, Sumida & Ichiro Yawata Foundation Scholarship in 2008, and R&D Excellence Scholarship from the Center for Wireless Information Technology in HKUST in 2006. He has served as an editorial assistant to the Editor-in-Chief of the IEEE Transactions on Communications since Jan. 2012. He is currently an Editor of the IEEE Communications Letters. He was a Co-Chair for the Wireless Access Track of 2014 IEEE 80th Vehicular Technology Conference. He has been a TPC member of various conferences, including the Globecom, WCNC, ICC, VTC, and PIMRC, etc. He was honoured as an Exemplary Reviewer of the IEEE Wireless Communications Letters for 2012, 2014.

Xiang-Gen Xia (M'97, S'00, F'09) received his B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, and his M.S. degree in mathematics from Nankai University, Tianjin, China, and his Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983, 1986, and 1992, respectively. He is currently the Charles Black Evans Professor, Department of Electrical and Computer Engineering, University of Delaware, Newark, Delaware, USA. Dr. Xia was the Kumars Chair Professor Group Professor (guest) in Wireless Communications, Tsinghua University, during 2009-2011, the Chang Jiang Chair Professor (visiting), Xidian University, during 2010-2012, and the WCU Chair Professor (visiting), Chonbuk National University, during 2009-2013. Dr. Xias current research interests include space-time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. He has over 280 refereed journal articles published and accepted, and 7 U.S. patents awarded and is the author of the book Modulated Coding for Intersymbol Interference Channels (New York, Marcel Dekker, 2000).

Dr. Xia received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He also received the Outstanding Junior Faculty Award of the Engineering School of the University of Delaware in 2001. He is currently serving and has served as an Associate Editor for numerous international journals including IEEE Transactions on Signal Processing, IEEE Transactions on Wireless Communications, IEEE Transactions on Mobile Computing, and IEEE Transactions on Vehicular Technology. Dr. Xia is Technical Program Chair of the Signal Processing Symp., Globecom 2007 in Washington D.C. and the General Co-Chair of ICASSP 2005 in Philadelphia. He is a Fellow of IEEE.

Chaowen Liu received the B.S. degree in electrical engineering from Henan University of Science and Technology, Luoyang, China, in 2011. He is currently working towards the Ph.D. degree at the Institute of Information Engineering, Xian Jiaotong University, Xian, China. His main research interests include node-positioning in wireless sensor networks, spatial domain modulation techniques in wireless MIMO communications, and physical layer security of wireless communications.