On Physical Layer Security: Weighted Fractional Fourier Transform based User Cooperation

Xiaojie Fang, *Student Member, IEEE,* Ning Zhang, *Member, IEEE,* Shan Zhang, *Member, IEEE,* Dajiang Chen, *Member, IEEE,* Xuejun Sha, *Member, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—In this paper, we propose a novel user cooperation scheme based on weighted fractional Fourier transform (WFRFT), to enhance the physical (PHY) layer security of wireless transmissions against eavesdropping. Specifically, instead of dissipating additional transmission power for friendly jamming, by leveraging the features of WFRFT, the information bearing signal of cooperators can create an identical *"artificial noise"* effect at the eavesdropper while causing no performance degradation on the legitimate receiver. Further, to form the cooperation set in an autonomous and distributed manner, we model WFRFT-based PHY-layer security cooperation problem as a coalitional game with non-transferable utility. A distributed merge-and-split algorithm is devised to facilitate the autonomous coalition formation to maximize the security capacity while accounting for the cooperation cost in terms of power consumption. We analyze the stability of the proposed algorithm and also investigate how the network topology efficiently adapts to the mobility of intermediate nodes. Simulation results demonstrate that the WFRFT-based user cooperation scheme leads to a significant performance advantage, in terms of secrecy ergodic capacity, compared with the conventional security-oriented user cooperation schemes, such as relay-jamming and cluster-beamforming.**

***Index Terms*—Physical layer security, weighted fractional Fourier transform (WFRFT), secrecy capacity, coalitional game theory.**

I. Introduction

ENSURING information security is of paramount importance for wireless communications. Due to the broadcast nature of radio propagation, any receiver within the cover range can listen and analyze the transmission without being detected, which makes wireless networks vulnerable to eavesdropping attacks. Traditionally, cryptographic algorithms/protocols implemented at upper layers of the open systems interconnection (OSI) protocol stack, have been widely used to prevent information disclosure to unauthorized users [1]. However, the layered design architecture with transparent physical layer leads to a loss in security functionality [2], especially for wireless communication scenarios where a common physical medium is always shared by both legitimate and non-legitimate users. Moreover, the cryptographic protocols can only offer a computational security [3]. The encryption algorithms could be compromised when the adversary has powerful computing capability, e.g. when quantum computing is available, most of the applied cryptography can be broken [4]. Most importantly, it is difficult to design an applicable secret key distribution and management protocol to satisfy the dynamic nature of wireless scenarios [5].

As an alternative, exploiting physical (PHY) layer characteristics for secure transmission has become an emerging hot topic in wireless communications [6–9]. The pioneering work by Wyner in [6] introduced the concept of *"secrecy capacity"* as a metric for PHY-layer security. Let X, Y, and Z be the input of the source, the outputs of the destination, and the eavesdropper, respectively. Then, *secrecy capacity* is defined by $\max[I(Y;X) - I(Z;X)]$, where $I(\cdot;\cdot)$ represents the mutual information. Specifically, the *secrecy capacity* characterizes the maximum rate at which message can be securely delivered. It is pointed out that perfect security is in fact possible without the aid of an encryption keys when the source-eavesdropper (wire-tap) channel is a degraded version of the source-destination (main) channel [6]. Taking uncertainty of wireless channels into consideration, the study on information-theoretic security is subsequently generalized to the Gaussian wiretap channels in [7] and the fading channels in [8], respectively. Triggered by the proliferation of multiple antenna systems, considerable research efforts towards developing multiple-input multiple-output (MIMO) techniques for PHY-layer security are devoted recently [10–12]. However, the feasibility of traditional PHY-layer security paradigms is hampered by the limitations of practical applications, i.e. secure information exchange can not be guaranteed when the wire-tap channel is stronger than the main channel, for which the secrecy capacity is typically zero under this scenario.

To overcome the above issues and improve attainable secrecy capacity, a multitude of sophisticated signal processing techniques have been developed to explore the extra degrees of freedom of MIMO systems for PHY-layer security. In [13–15], security-oriented beamforming is employed, whereby the transmitter constructs the transmission signal dedicated for the destination, leading to a secrecy capacity improvement. In [16–18], a sort of specific signals with nulls directed towards the destination, termed as *"artificial noise"*, are generated to eliminate information leakage. In [19], the optimal

X. Fang is with the Department of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China and the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1, Canada. (e-mail: fangxiaojie@hit.edu.cn; x33fang@uwaterloo.ca).

N. Zhang, S. Zhang and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1, Canada (e-mail: n35zhang@uwaterloo.ca; zhangshan_2011@outlook.com; sshen@uwaterloo.ca).

D. Chen is with the School of information and software engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China and the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1, Canada. (e-mail: djchen@uestc.edu.cn).

X. Sha is with the Department of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: shaxuejun@hit.edu.cn).

Manuscript received June 1, 2017.

power allocation/sharing problem between the information signal and the artificial noise is studied. Due to the resource limitations of wireless terminals, user cooperation is further proposed as a practical strategy to harvest the multiple antenna gains [20–22]. The work in [14, 20] investigate the cooperative beamforming design problem by exploring the optimal relay selection for secrecy capacity maximization, under both decode-and-forward (DF) and amplify-andforward (AF) modes, respectively. In [21, 23], friendly jammers are deployed for generating *"artificial noise"* to defend against eavesdropping attacks. Generally, the ultimate objective of beamforming or *"artificial noise"* is to boost the secrecy rate of the main channel by decreasing the leakage rate of the wiretap channel. However, most of existing beamforming techniques could be compromised to powerful adversaries that equipped with high-performance antenna (arrays). Typically, only quadratic antenna resources are required for eavesdroppers to have a competitive chance at undermining the secret communication of the main channel [24]. Although inserting *"artificial noise"* can mitigate the information leakage, it incurs the cost of wasting valuable transmission power, since a certain amount of the transmission energy has to be assigned to the *"artificial noise"*. To warp up, we pose the following question: *is it possible that the information bearing signal can be designed as the "artificial noise" to confound the eavesdropper while imposing no impact on the legitimate receiver?* One potential solution to this question is Weighted fractional Fourier Transform (WFRFT). WFRFT, known as a novel time-frequency analyzing tool, has drawn gradual attention in wireless communications recently. The concept of WFRFT-based communication system is pioneeringly proposed by [25], where WFRFT is recognized as a hybrid modulation scheme of weighted single-carrier (SC) and multi-carrier (MC) modulation. Explicitly, the compatible process of SC and MC modulation makes it feasible for a WFRFT-based system to adjust its the signal distribution to adapt to different communication scenarios. With this favorable property, WFRFT has manifested itself a promising solution for interference suppression [26–30].

In this paper, we aim to investigate the superiority and practicability of WFRFT from the PHY-layer security perspective. To the best of our knowledge, this is the first work that utilizes the WFRFT theory to facilitate the PHY-layer security through cooperation. The WFRFT signal, in fact, is a weighted combination of multiple different signals bearing the identical information. More specifically, WFRFT operations with different parameters result in distinct outputs that can only be recovered through the corresponding inverse-WFRFT operations, i.e. the orthogonality of each sub-signal has to be guaranteed. By exploring those features, we attempt to generalize beamforming signal and artificial noise to enhance the secrecy without any impact on the destination. Moreover, we consider user cooperation for further secrecy enhancement, where each intermediate user decodes and forwards the source message with WFRFT techniques. Pre-equalization is employed such that the signal combination of multiple relays can be reliably decoded by the destination. Taking the wireless channel uncertainty into account, the eavesdropper only receives a degraded version of the transmitted signals, even if the wiretap channel is much stronger than the main channel. The reason is that interference between sub-signals occurs when their orthogonality is broken, leading to an *"artificial noise"* effect. To stimulate and select suitable cooperators, a distributed coalitional game strategy is further proposed. As selfish and rational player, each intermediate user is rewarded according to its contribution. To find the distributed solution, we proposed a Merge-and-Split based algorithm that allows each user to autonomously join or leave a coalition. The proposed algorithm is proved to converge to a Nash-stable coalitional structure. Simulation results are provided to evaluate the performance of the WFRFT-based PHY-layer security cooperation scheme.

The remainder of this paper is organized as follows: Mathematical precepts of WFRFT are presented in Section II. The system model and formulation of the WFRFT-based user cooperation for PHY-layer security are given in Sections III and IV, respectively. In Section V, the proposed distributed coalitional game is formulated and solved. Simulation results are provided in Section VI. Finally, Section VII concludes this paper.

II. Weighted Fractional Fourier Transform

Weighted Fractional Fourier Transform, a generalization of the Fourier Transform (FT), is a promising techinique for signal and image processing. In this section, we introduce the basic definitions and properties of WFRFT, based on which WFRFT-based PHY-layer security technique will be developed in the subsequent sections.

Definition 1: Given an arbitrary complex vector $\mathbf{X} := [x_0, ..., x_{N-1}] \in \mathbb{C}^N$, the α-order WFRFT of $\mathbf{X}$, $\mathscr{F}^{\alpha}(\mathbf{X})$, is defined by[1]:

$$\mathscr{F}^{\alpha}(\mathbf{X}) = \mathfrak{F}_M^{\alpha}[\mathbf{X}] = \sum_{l=0}^{M-1} A_l(\alpha)\mathbf{T}^{\frac{4l}{M}}\mathbf{X}, \tag{1}$$

where $\mathbf{T}$ represents the WFRFT kernel (or basic operator), while $M \in \mathbb{Z}^+; M \geq 4$ indicates the number of the basic operators involved. Moreover, the weighting coefficients $\{A_l(\alpha)\}_{l=0}^{M-1}$ are generated by

$$A_l(\alpha) = \frac{1}{M}\frac{1-\exp\left[-2\pi j(\alpha-l)\right]}{1-\exp\left[-2\pi j(\alpha-l)/M\right]}. \tag{2}$$

In particular, we refer to M-WFRFT as α-order WFRFT operator consisting of M basic transforms, and denote it by $\mathfrak{F}_M^{\alpha}$. For briefness, we define $\mathbf{W}_M^{\alpha} = \sum_{l=0}^{M-1} A_l(\alpha)\mathbf{T}^{\frac{4l}{M}}$ as the α-order M-WFRFT matrix.

Definition 2: The WFRFT kernel $\mathbf{T}$ is a finite recursive combination of the state functions of the conventional FT and satisfies the following axioms:

- *Unitary axiom*: $\mathfrak{F}_M^{\alpha}\left[\mathfrak{F}_M^{-\alpha}[\mathbf{X}]\right] = \mathbf{X}$, $\{\mathbf{W}_M^{\alpha}\}^H = \mathbf{W}_M^{-\alpha}$;
- *Boundary axiom*: $\mathfrak{F}_M^{0}[\mathbf{X}] = \mathbf{X}$, $\mathfrak{F}_M^{1}[\mathbf{X}] = DFT(\mathbf{X})$;
- *Additive axiom*: $\mathfrak{F}_M^{\alpha+\beta}[\mathbf{X}] = \mathfrak{F}_M^{\alpha}\left[\mathfrak{F}_M^{\beta}[\mathbf{X}]\right] = \mathfrak{F}_M^{\beta}\left[\mathfrak{F}_M^{\alpha}[\mathbf{X}]\right]$.

[1]For better understanding, this paper defines the WFRFT in a discrete form, the continuous WFRFT definition can be found in [31].

Without loss of generality, we utilize the classical-WFRFT (CWFRFT) as the basic operator of M-WFRFT. In what follows, we will provide the relevant basic theorems.

Let $\boldsymbol{I}$ denote an $N\times N$ identify matrix and $\boldsymbol{F}$ denote an N-point normalized Fourier matrix with (n,k)-th element satisfying $[\boldsymbol{F}]_{n,k} = (1/\sqrt{N})\cdot\exp(-j2\pi nk/N)$.

Definition 3: The α-order CWFRFT of an arbitrary complex vector $\mathbf{X} := [x_0, ..., x_{N-1}] \in \mathbb{C}^N$ is defined by

$$\mathscr{F}_c^{\alpha}(\mathbf{X}) = (w_0^{\alpha}\boldsymbol{I} + w_1^{\alpha}\boldsymbol{F} + w_2^{\alpha}\boldsymbol{F}^2 + w_3^{\alpha}\boldsymbol{F}^3)\boldsymbol{X}, \tag{3}$$

where the coefficients $\{w_p^{\alpha}\}_{p=0}^{3} = \frac{1}{4}\sum_{k=0}^{3}\exp\left\{\frac{-2\pi j(\alpha-p)k}{4}\right\}$.

Property 1: The CWFRFT has a periodicity of 4:

$$\mathscr{F}_c^{\alpha+4}(\mathbf{X}) = \mathscr{F}_c^{\alpha}(\mathbf{X}), \tag{4}$$

Property 2: When $a \in \mathbb{Z}$, the CWFRFT degenerates into the conventional FT:

$$\mathscr{F}_c^{\alpha}(\mathbf{X}) = \boldsymbol{F}^{\alpha}\cdot\mathbf{X}, \tag{5}$$

Property 3: For real a and b, the additive property holds:

$$\mathscr{F}_c^{\alpha+b}(\mathbf{X}) = \mathscr{F}_c^{a}\left(\mathscr{F}_c^{b}(\mathbf{X})\right) = \mathscr{F}_c^{b}\left(\mathscr{F}_c^{a}(\mathbf{X})\right), \tag{6}$$

For proofs of these properties, please refer to Appendix A. ■

Theorem 1: Let CWFRFT be the basic operator of M-WFRFT, and M-WFRFT degrades to CWFRFT when $M = 4$.

Proof: Let $\mathbf{T} = (w_0^{\alpha}\boldsymbol{I} + w_1^{\alpha}\boldsymbol{F} + w_2^{\alpha}\boldsymbol{F}^2 + w_3^{\alpha}\boldsymbol{F}^3)$ be the basic operator, and set $M = 4$. With *Property 2*, we have

$$\mathfrak{F}_4^{\alpha}[\mathbf{X}] = \sum_{l=0}^{3}A_l(\alpha)\mathbf{T}^l\mathbf{X} = \sum_{l=0}^{3}A_l(\alpha)\boldsymbol{F}^l\mathbf{X}. \tag{7}$$

In addition, when $M = 4$, $\{A_l(\alpha)\}_{l=0}^{3}$ we have:

$$A_l(\alpha) = \frac{1}{4}\sum_{k=0}^{3}\exp\left\{\frac{-2\pi j(\alpha-l)k}{4}\right\}. \tag{8}$$

Thus, the proof is completed. ■

Theorem 2: Let α_4 and α_M be the parameters of 4-WFRFT and M-WFRFT, respectively. Then, $\mathbf{W}_4^{\alpha_4} = \mathbf{W}_M^{\alpha_M}$ holds for $\alpha_M = \frac{M}{4}\alpha_4$, and *vice versa*.

Proof: Please refer to Appendix B. ■

By aforementioned theorems and properties, it is true that $\mathfrak{F}_M^{\alpha}$ satisfies all of the axioms in Definition 2, when $\mathbf{T} = \sum_{l=0}^{4}A_l(\alpha)\boldsymbol{F}^l$.

Theorem 3: $\mathbf{W}_M^{\alpha}\cdot\mathbf{W}_M^{\beta} = \boldsymbol{I}$, iff $\alpha+\beta = 0$ and the weighting coefficients $\{A_l(\alpha)\}_{l=0}^{M-1}$ and $\{A_l(\beta)\}_{l=0}^{M-1}$ are not contaminated.

Proof: Please refer to Appendix C. ■

Remark 1: M-WFRFT can split the input signal into M signal components with weights $\{A_l(\alpha)\}_{l=0}^{M-1}$, which is similar to the functionality of resource allocation.

Remark 2: Theorem 2 provides an unified decoding strategy for M-WFRFT. The basic 4-WFRFT demodulator can be used to demodulate any M-WFRFT signal properly. Therefore, no matter how does the transmitter structure change, the receiver can remain unchanged. Theorem 3 suggests that the orthogonality in signal components directly determines the decoding performance, which is the most fundamental property leveraged by the WFRFT-based PHY-layer security scheme for information privacy preserving.

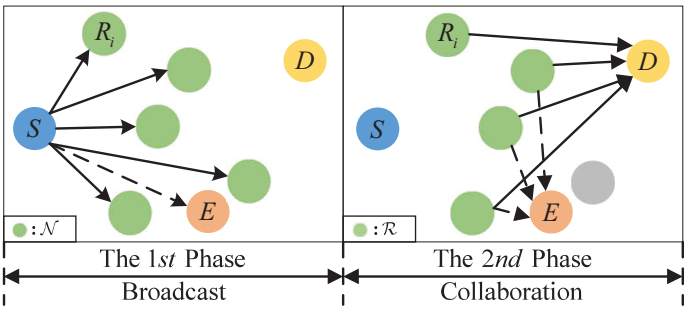


Fig. 1. The cooperative multiuser relay system model.

III. System Model

As depicted in Fig. 1, we consider a cooperative system consisting of one source (S), one destination (D), and N trustful intermediate nodes ($\{R_i\}_{i=1}^{N}$), in the presence of an eavesdropper (E) who attempts to eavesdrop on the source information. There is no direct link between S and D [14, 20], e.g., the direct link between source and destination ($S \to D$) is blocked by an obstacle. S aims to transmit information securely to D, with the aid of intermediate nodes. All nodes are equipped with one single antenna and operate in a half-duplex mode. The system operation is performed in a two-phase fashion. In the first phase, the source broadcasts its signal to the N trustful intermediate nodes among which the nodes that can successfully decode the source signal form a collaboration set $\boldsymbol{\mathcal{R}}$.[2] In the second phase, the intermediate nodes perform WFRFT operation to forward a converted version of the source message to D, to boost the secrecy rate of the S-D link. In particular, only those that form the optimal coalition with best security performance are selected to forward their received signals.[3] To concentrate on the intermediate nodes collaboration, we assume the links $S \to R_i, \forall R_i \in \boldsymbol{\mathcal{R}}$ are secure, similar to [20, 21, 32, 33].

Without loss of generality, a quasi-static block Rayleigh fading environment is considered, and the thermal noise is characterized by a complex Gaussian variable with zero mean and variance σ_n^2. The fading coefficients of link $S \to R_i$, $S \to E$, $R_i \to D$, $R_i \to E$, $(\forall R_i \in \boldsymbol{\mathcal{R}})$ are denoted by h_s^i, h_{se}, h_d^i, h_e^i, respectively. Similar to [14] and [15], the CSI of both main and wiretap channels are assumed available, which is a typical assumption in the PHY-layer security literature. Moreover, we consider the worst case where the eavesdropper knows everything about the signal transmission in the link $S \to R_i \to D$, including the knowledge of WFRFT, the encoding paradigm at S, the decoding, re-encoding and the forwarding (DEF) protocols at R_i, and decoding method at D. Moreover, all intermediate nodes are considered to have the ability to perform 4- WFRFT (De)-modulation operation. In what follows, we analytically show how WFRFT can be cooperatively performed among multiple intermediate nodes for PHY-layer security enhancement.

[2]Node $R_i \in \boldsymbol{\mathcal{R}}, \forall i \in \{1, 2, ..., N\}$ if $C_{sec}^i \geq \mathbf{R}_0$, where C_{sec}^i is the secrecy capacity of link $S \to R_i$ and $\mathbf{R}_0$ is the transmission rate of S.

[3]The strategy of choosing optimal intermediate nodes for the two-phase cooperation is explicitly explained in Section IV.

Throughout this paper, $[x]^+ \triangleq \max\{x, 0\}$; $\mathbf{E}[\cdot]$ is the expectation operator; $\log(\cdot)$ denotes the base-2 logarithm; $\|\cdot\|$ denotes the Euclidean norm; $|\cdot|$ represents the cardinality of a set; $x^\star$ picks the optimal value of x; and superscripts $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ represent the conjugate, transpose and conjugate transpose, respectively.

IV. PHY-layer security via WFRFT-based User Cooperation

Following the existing PHY-layer security literature, we use *secrecy capacity* to evaluate the performance of a PHY-layer security scheme. Basically, secrecy capacity upper bounds the maximum achievable rate of link $S \to \boldsymbol{\mathcal{R}} \to D$ while leaking no information to E.

Consider an N intermediate nodes network $\boldsymbol{\mathcal{N}} := \{R_i | i = 1, ..., N\}$, during the broadcast phase, the transmitter contrives to form an initial coalition pool $\boldsymbol{\mathcal{R}} \subset \boldsymbol{\mathcal{N}}$, which includes all nodes that can decode the transmission securely. Assume that *artificial noise* injection strategy has been performed, then $\boldsymbol{\mathcal{R}}$ can be generated by:

$$\begin{aligned} &\forall R_i \in \boldsymbol{\mathcal{R}} \\ s.t. \quad & C_{sec}^i \geq \mathbf{R}_0;\ C_{sec}^i = \left[C_{sr}^i - C_{se}\right]^+, \\ & C_{sr}^i = \log\left(1 + \frac{P_0 ||h_s^i||^2}{\sigma_n^2}\right); \\ & C_{se} = \log\left(1 + \frac{P_0 ||h_{se}||^2}{\sum\limits_{R_j \in \boldsymbol{\mathcal{N}}} P_j ||h_e^j||^2 + \sigma_n^2}\right), \\ & R_i \neq R_j;\ R_i, R_j \in \boldsymbol{\mathcal{N}}, \end{aligned} \tag{9}$$

where $\mathbf{R}_0$ is the source transmission rate; C_{sr}^i and C_{se} characterize the channel capacity of link $S \to R_i$ and $S \to E$, respectively. P_0 and P_j denote the transmission power of the source and the intermediate node (jammer) R_j, respectively. Note that *artificial noise* based PHY-layer security is a well developed technique, following the existing research results, $\boldsymbol{\mathcal{R}}$ can be reliably obtained. In particular, the *artificial noise* injection strategy of (9) can be achieved by a set of iteration procedures expressed by Algorithm 1.

In the collaboration phase, the intermediate nodes in $\boldsymbol{\mathcal{R}}$ cooperatively relay the source message to D using DEF protocol. In particular, each intermediate node performs as a basic operator of WFRFT, and only the optimal combination $\boldsymbol{\mathcal{R}}^\star$ will be selected to re-encode and transmit their decoded outcome to D. For an arbitrary combination $\boldsymbol{\mathcal{C}}$ the signal transmitted from the $R_i (R_i \in \boldsymbol{\mathcal{C}})$ is given by,

$$y_i = \lambda_i A_i(\alpha) \mathfrak{F}_4^{\frac{4i}{|\boldsymbol{\mathcal{C}}|}} [\mathbf{X}], \tag{10}$$

where λ_i represents the pre-equalization factor. Denote $\mathbf{y} = [y_1, y_2, ...y_{|\boldsymbol{\mathcal{C}}|}]^T$, $\mathbf{h}_{rd} = [h_d^1, h_d^2, ...h_d^{|\boldsymbol{\mathcal{C}}|}]$ and $\mathbf{h}_{re} = [h_e^1, h_e^2, ...h_e^{|\boldsymbol{\mathcal{C}}|}]$. Note that, h_d^i and h_e^i represent the complex channel coefficients from node R_i to D and E, respectively, where $i \in \{1, 2, ..., |\boldsymbol{\mathcal{C}}|\}$. Then, the received signals r_D and r_E at D and E in the collaboration phase can be written respectively:

$$\begin{aligned} r_D &= \mathbf{h}_{rd}\mathbf{y} + n_0 = \sum_{i=0}^{|\boldsymbol{\mathcal{C}}|} h_d^i \lambda_i A_i(\alpha) \mathfrak{F}_4^{\frac{4i}{|\boldsymbol{\mathcal{C}}|}} [\mathbf{X}] + n_{rd} \\ r_E &= \mathbf{h}_{re}\mathbf{y} + n_0 = \sum_{i=0}^{|\boldsymbol{\mathcal{C}}|} h_e^i \lambda_i A_i(\alpha) \mathfrak{F}_4^{\frac{4i}{|\boldsymbol{\mathcal{C}}|}} [\mathbf{X}] + n_{re}. \end{aligned} \tag{11}$$

where n_{rd} and n_{re} are the thermal noise at D and E, respectively. Based upon **Theorem 3**, when $\boldsymbol{\lambda} := [\lambda_1, \lambda_2 ..., \lambda_{|\boldsymbol{\mathcal{C}}|}]^T$ is an amplitude&phase pre-equalization vector satisfying $\lambda_i = (h_d^i)^* / \left\|h_d^i\right\|^2$, the cooperation can facilitate the reception at D. The achievable rate at D can be expressed as follows:

$$C_{rd} = \log\left(1 + \frac{\sum_{i=0}^{|\boldsymbol{\mathcal{C}}|} \|A_i(\alpha)\|^2 P_0}{\sigma_n^2}\right). \tag{12}$$

Whereas at the eavesdropper E, the orthogonality between the signal components from different intermediate nodes are contaminated. Assume that β-order 4-WFRFT is performed by E,[4] then the signal to interference plus noise ratio (SINR) γ_{re}^i at R_i is a straightforward result of [34]:

$$\gamma_{re}^i = \frac{\left\|\kappa^i\right\|^2 \left\|h_e^i \lambda_i A_i(\alpha)\right\|^2 P_0}{\left(1 - \left\|\kappa^i\right\|^2\right) \left\|h_e^i \lambda_i A_i(\alpha)\right\|^2 P_0 + \sigma_n^2}, \tag{13}$$

Algorithm 1 Artificial noise injection Algorithm for the secure broadcast phase

Stage I: Initial State

Initially, each node in $\boldsymbol{\mathcal{N}}$ reports its current states to the network, including available power consumption, channel state information, etc..

Stage II: Initial Coalition Pool Formation

LOOP

Phase 1:

S checks the network status and selects R_i as the temporary relay node.

Phase 2:

S calculates C_{sr}^i and C_{se} to check whether node R_i satisfies the constraint $C_{sec}^i \geq \mathbf{R}_0$

Phase 3:

IF $C_{sec}^i \geq \mathbf{R}_0$ **THEN**

S add node R_i into the initial coalition pool $\boldsymbol{\mathcal{R}}$; Meanwhile, S send the source message to R_i and other intermediate nodes $R_i \neq R_j; R_j \in \boldsymbol{\mathcal{N}}$ generates the artificial noise to selectively degrade eavesdropper's reception.

ELSE

break;

Untill All nodes in $\boldsymbol{\mathcal{N}}$ have been checked, S completes the construction of the initial coalition pool $\boldsymbol{\mathcal{R}}$

[4]According to **Definition 1**, the received signal at E is the mixture of $|\boldsymbol{\mathcal{C}}|$ different 4-WFRFT signals. There is no way for E to rule out the mutual-interference, when the orthogonality of the signal components is damaged.

where $\kappa^i = w_0^{(\frac{4i}{|\mathcal{C}|}+\beta)}$ determines the information leakage from R_i to E while w_0 is the weighting coefficient of 4-WFRFT. Then the achievable rate at E can be expressed by [14]:

$$C_{re} = \log\left(1 + \sum_{i=0}^{|\mathcal{C}|} \gamma_{re}^i\right). \tag{14}$$

Combining (12) and (14), the secrecy capacity with WFRFT-based cooperation is given by:

$$\begin{aligned} C_{sec} &= [C_{rd} - C_{re}]^+ \\ &= \left[\log\left(1 + \frac{\sum_{i=0}^{|\mathcal{C}|} \|A_i(\alpha)\|^2 P_0}{\sigma_n^2}\right)\right. \\ &\quad \left. - \log\left(1 + \sum_{i=0}^{|\mathcal{C}|} \frac{\left\|\kappa^i\right\|^2 \left\|h_e^i \lambda_i A_i(\alpha)\right\|^2 P_0}{(1-\|\kappa^i\|^2)\|h_e^i \lambda_i A_i(\alpha)\|^2 P_0 + \sigma_n^2}\right)\right]^+ \end{aligned} \tag{15}$$

The objective of employing cooperation is to maximize the overall secrecy capacity. However, as rational players, the intermediate nodes might not cooperate unconditionally. To stimulate cooperation, an appropriate amount of reward can be paid for the intermediate nodes. With this regard, the problem of selecting suitable cooperators can be formulated as follows:

$$\begin{aligned} \boldsymbol{\mathcal{R}}^\star &= \underset{\boldsymbol{\mathcal{C}} \subseteq \boldsymbol{\mathcal{R}}}{\operatorname{argmax}} \left[\eta C_{sec} - \sum_{R_i \in \boldsymbol{\mathcal{C}}} \xi_i P_s^i\right] \\ s.t. \quad & P_s^i \le P_a^i, \forall R_i \in \boldsymbol{\mathcal{C}} \text{ and } C_{sec} > \mathbf{R}_0, \end{aligned} \tag{16}$$

where η is the profit per secrecy rate, ξ_i is the cooperation cost per unit power consumption of R_i. P_s^i and P_a^i represent the total power consumption and the available power budget of R_i during each transmission.

The optimal cooperator set can be determined such that the best secrecy performance is achieved at the lowest cost. Intuitively, to find $\boldsymbol{\mathcal{R}}^\star$, an exhaustive search can be applied. However, finding the optimal cooperator set via an exhaustive search is a non-deterministic polynomial (NP)-complete problem. The possible cooperation structures will grow exponentially with the number of intermediate nodes in $\boldsymbol{\mathcal{R}}$. Moreover, the complexity further increases because of the fact that the overall PHY-layer secrecy rate C_{sec} and the system cost $\sum_{R_i \in \boldsymbol{\mathcal{C}}} \xi_i P_s^i$ varies for different coalitions. Therefore, it is desirable to have a highly efficient means to form a stable cooperation.

V. Coalition Formation and Solution

In this section, we model the user cooperation among the intermediate nodes as a coalitional game [35–37] to select the optimal cooperators for the WFRFT-based PHY-layer security scheme.

A. Coalition Formation

Definition 4: The coalitional form of an N-player game with non-transferable utility (NTU) is defined by $(\boldsymbol{\mathcal{N}}, V)$, where $\boldsymbol{\mathcal{N}} := \{R_i | i = , 1, ..., N\}$ represents the set of players and $V(\boldsymbol{\mathcal{S}})$ personifies the value of coalition $\boldsymbol{\mathcal{S}}; \boldsymbol{\mathcal{S}} \subset \boldsymbol{\mathcal{N}}$.

In this paper, the intermediate nodes are regarded as the players and coalition $\boldsymbol{\mathcal{S}}$ denotes the group of intermediate nodes that cooperatively relay the source message via a $|\boldsymbol{\mathcal{S}}|$-WFRFT mechanism. Without loss of generality, consider an arbitrary coalition $\boldsymbol{\mathcal{S}} := \{R_1, R_2, ..., R_{|\boldsymbol{\mathcal{S}}|}\} \subseteq \boldsymbol{\mathcal{N}}$ and its coalition value is defined as follows:

$$\begin{aligned} V(\boldsymbol{\mathcal{S}}) = \{\boldsymbol{\phi}(\mathcal{S}) \in \mathbb{R}^{|\boldsymbol{\mathcal{S}}|} | \ \forall R_i \in \boldsymbol{\mathcal{S}}, \phi_i(\boldsymbol{\mathcal{S}}) = [v_i(\boldsymbol{\mathcal{S}}) - u_i(\boldsymbol{\mathcal{S}})]^+ \\ \text{for } P_s^i \le P_a^i, \text{ and } \phi_i(\boldsymbol{\mathcal{S}}) = -\infty \text{ otherwise.}\}, \end{aligned} \tag{17}$$

where $v_i(\boldsymbol{\mathcal{S}}) = C_{sec}^{\boldsymbol{\mathcal{S}}} - C_{sec}^{\boldsymbol{\mathcal{S}}-R_i}$ denotes the PHY-layer secrecy capacity gain for node $R_i \in \boldsymbol{\mathcal{S}}$ given by (15) under the constraint $P_s^i \le P_a^i$ while $u_i(\boldsymbol{\mathcal{S}}) = \xi_i P_s^i$ is the payoff that quantifies the cost when node $R_i \in \boldsymbol{\mathcal{S}}$. Generally, (17) evaluates the benefits obtained from cooperation, in terms of the PHY-layer secrecy gain, taking into account the cost or payoff to stimulate the intermediate nodes.

In the WFRFT-based PHY-layer security cooperation scheme, the source S acts as the "buyer" who pays an amount of reward for the "service" provided by the intermediate nodes $R_i \in \boldsymbol{\mathcal{N}}$, in order to achieve a secure information exchange with D. Note that, only the optimal coalition $\boldsymbol{\mathcal{R}}^\star$ will be chosen for data transmission. Therefore, there is a competition among the intermediate nodes to participate into the coalition for the reward. Subsequently, the WFRFT-based PHY-layer security cooperation problem can be formulated by a coalitional game as follows:

Proposition 1: The WFRFT-based PHY-layer security coalitional game is a $(\boldsymbol{\mathcal{N}}, V)$ NTU game.

proof: Proposition 1 is an immediate result of the fact that the coalition value of coalition $\boldsymbol{\mathcal{S}} \subseteq \boldsymbol{\mathcal{N}}$ given in (17) relies on how the players in the coalition are structured. Specifically, the coalition value of the game is a set of benefit vectors, $\boldsymbol{\phi}(\boldsymbol{\mathcal{S}}) \in \mathbb{R}^{|\boldsymbol{\mathcal{S}}|}$, whose element $\phi_i(\boldsymbol{\mathcal{S}})$ indicates the benefits that can obtain by absorbing R_i member of $\boldsymbol{\mathcal{S}}$. Consequently, the WFRFT-based PHY-layer security coalitional game has a non-transferable utility. ■

Definition 5: The coalitional game with NTU is super-additive if and only if:

$$\begin{aligned} V(\boldsymbol{\mathcal{S}}) \supseteq \{\boldsymbol{\phi}(\boldsymbol{\mathcal{S}}) \in \mathbb{R}^{|\boldsymbol{\mathcal{S}}|} | \phi_i(\boldsymbol{\mathcal{S}}_1) \in V(\boldsymbol{\mathcal{S}}_1); \ \phi_j(\boldsymbol{\mathcal{S}}_2) \in V(\boldsymbol{\mathcal{S}}_2) \\ \forall \boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2 \subset \boldsymbol{\mathcal{N}}; \boldsymbol{\mathcal{S}}_1 \cup \boldsymbol{\mathcal{S}}_2 = \boldsymbol{\mathcal{S}}; \boldsymbol{\mathcal{S}}_1 \cap \boldsymbol{\mathcal{S}}_2 = \emptyset\}. \end{aligned} \tag{18}$$

Proposition 2: The WFRFT-based PHY-layer security coalitional game $(\boldsymbol{\mathcal{N}}, V)$ is a non-superadditive game.

proof: Consider two disjoint coalitions $\boldsymbol{\mathcal{S}}_1$ and $\boldsymbol{\mathcal{S}}_2$, satisfying $\boldsymbol{\mathcal{S}} = \boldsymbol{\mathcal{S}}_1 \cup \boldsymbol{\mathcal{S}}_2$. The non-superadditive of the WFRFT-based PHY-layer security coalitional game can be proved by checking:

$$V(\boldsymbol{\mathcal{S}}) \not\supseteq \{\boldsymbol{\phi}(\boldsymbol{\mathcal{S}}) \in \mathbb{R}^{|\boldsymbol{\mathcal{S}}|} | \phi_i(\boldsymbol{\mathcal{S}}_1) \in V(\boldsymbol{\mathcal{S}}_1); \phi_j(\boldsymbol{\mathcal{S}}_2) \in V(\boldsymbol{\mathcal{S}}_2)\}. \tag{19}$$

Consider a special case in which coalition $\boldsymbol{\mathcal{S}}_1$ achieves an extreme high secrecy rate while coalition $\boldsymbol{\mathcal{S}}_2$ is with low secrecy rate. This case can be typically found when players in $\boldsymbol{\mathcal{S}}_1$ and $\boldsymbol{\mathcal{S}}_2$ are at proximate of the destination and eavesdropper, respectively. Assume $R_j \in \boldsymbol{\mathcal{S}}_2$ is with positive coalition value $\phi_j(\boldsymbol{\mathcal{S}}_2)$. Clearly, when $\boldsymbol{\mathcal{S}}_1$ and $\boldsymbol{\mathcal{S}}_2$ are merged, $C_{sec}^{S_1+R_j} - C_{sec}^{S_1} <= 0$, which means the overall secrecy rate

of the coalition is degraded. In this case, $\phi_j(\boldsymbol{\mathcal{S}}_1 \cup \boldsymbol{\mathcal{S}}_2) < 0$, i.e. R_j's coalition value would be 0 in the merged coalition $\boldsymbol{\mathcal{S}}$. However, in the original coalition $\boldsymbol{\mathcal{S}}_2$, R_j's coalition value is positive, which does not belong to $V(\boldsymbol{\mathcal{S}})$. Therefore, the WFRFT-based PHY-layer security coalitional game is non-superadditive. ■

The non-superadditive property implies that the coalitions with more participants may not be always beneficial. That is because the benefits provided by a coalition, in terms of secrecy capacity, would be limited by the cost associated. In this regard, the coalition with huge number of intermediate nodes are not optimal and will not be formed. Instead, in the proposed scenario, multiple disjoint coalitions will form and the one with best secrecy performance is selected as the ultimate coalition set. To this end, a distributive algorithm is proposed to form the disjoint coalitions, which is elaborated in the following subsection.

B. Coalition Algorithm

In this subsection, we design an algorithm to achieve autonomous coalition formation for the WFRFT-based PHY-layer security cooperation problem.

Definition 6: A coalitional structure is referred to as a *collection*, if $\boldsymbol{\mathcal{L}} := \{\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, ...\boldsymbol{\mathcal{S}}_L | \ \forall i, j \in 1, 2, ...L, i \neq j, \boldsymbol{\mathcal{S}}_i \cap \boldsymbol{\mathcal{S}}_j = \emptyset$ and $\boldsymbol{\mathcal{S}}_i \cup \boldsymbol{\mathcal{S}}_j \subseteq \boldsymbol{\mathcal{N}}\}$. Typically, a *collection* that satisfies $\bigcup_{i=1}^{l} \boldsymbol{\mathcal{S}}_i = \boldsymbol{\mathcal{N}}$, is referred to as a *partition* of $\boldsymbol{\mathcal{N}}$. Note that, a partition is not necessarily formed.

For an N-players coalitional game, there exists $2^N - 1$ nonempty coalitions which can form B_N different *collections*, where B_N is the N-th Bell number, given by:

$$B_N = \sum_{i=0}^{N-1} \binom{N-1}{i} B_i, \text{ for } N \geq 1 \ B_0 = 1. \tag{20}$$

Let $\boldsymbol{\mathcal{S}}_l$ be an arbitrary coalition, and a player's action is to decide whether to be a member of $\boldsymbol{\mathcal{S}}_l$ according to its status in the group, namely its contribution to the group in term of secrecy rate gain, and its expected payoff. Since the players are rational, the designation of the players into suitable coalitions is performed according to following criteria.

Definition 7: Consider two *collections* $\boldsymbol{\mathcal{L}} := \{\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, ...\boldsymbol{\mathcal{S}}_L\}$ and $\boldsymbol{\mathcal{P}} := \{\boldsymbol{\mathcal{S}}_1^*, \boldsymbol{\mathcal{S}}_2^*, ...\boldsymbol{\mathcal{S}}_K^*\}$ that partition the same set $\boldsymbol{\mathcal{R}} \subseteq \boldsymbol{\mathcal{N}}$. Then, we use the symbol $\succ$ to represent their comparison relation. Specifically, $\boldsymbol{\mathcal{L}} \succ \boldsymbol{\mathcal{P}}$ implies that the way $\boldsymbol{\mathcal{L}}$ partitions $\boldsymbol{\mathcal{R}}$ outperforms the way $\boldsymbol{\mathcal{P}}$ partitions $\boldsymbol{\mathcal{R}}$.

In order to achieve a rational and stable coalition, a multitude of comparison orders, based on both coalition utility and individual payoff, have been introduced in existing works[35, 36]. In particular, a comparison order, such as the *utilitarian order*, is coalition rational if $\boldsymbol{\mathcal{L}} \succ \boldsymbol{\mathcal{P}} \Leftrightarrow \sum_{i=1}^{L} V(\boldsymbol{\mathcal{S}}_i) \geq \sum_{i=1}^{K} V(\boldsymbol{\mathcal{S}}_i^*)$. On the contrary, a comparison order is regarded as individual rational, such as the *Pareto order*, if:

$$\boldsymbol{\mathcal{L}} \succ \boldsymbol{\mathcal{P}} \Leftrightarrow \left\{ \begin{array}{ll} \forall R_i \in \boldsymbol{\mathcal{R}}, & \phi_i(\boldsymbol{\mathcal{L}}) \geq \phi_i(\boldsymbol{\mathcal{P}}) \\ \exists R_i \in \boldsymbol{\mathcal{R}}, & \phi_i(\boldsymbol{\mathcal{L}}) > \phi_i(\boldsymbol{\mathcal{P}}), \end{array} \right\} \tag{21}$$

which indicates that $\boldsymbol{\mathcal{L}}$ is superior to $\boldsymbol{\mathcal{P}}$ iff at least one player can achieve more benefits by changing the partition structure from $\boldsymbol{\mathcal{L}}$ to $\boldsymbol{\mathcal{P}}$, without degrading other players' benefits.

Algorithm 2 Merge-and-Split Coalition Formation Algorithm for WFRFT-based Collaborative PHY-layer Security

Stage I: Initial State

Initially, S broadcasts the information to nearby nodes. Suppose that there exists an initial set $\boldsymbol{\mathcal{R}}$, consisting of L suitable nodes. Set the initial partition state as $\boldsymbol{\mathcal{L}} := \{\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, ...\boldsymbol{\mathcal{S}}_L\}$.

Stage II: Coalition Formation Algorithm

Phase 1: Neighbor nodes discovering

Each node in $\boldsymbol{\mathcal{R}}$ reports its available power consumption to the network, and checks the network status to find candidate partners.

Phase 2: Dynamic coalition construction

Set intermediate nodes into cooperating mode, and initialize the collaborator list of each node as NULL.

LOOP

a) $\boldsymbol{\mathcal{L}}' = Merge(\boldsymbol{\mathcal{L}})$, merge any disjoint collisions in $\boldsymbol{\mathcal{L}}$ that meets the *Merge rule*.

b) $\boldsymbol{\mathcal{L}}'' = Split(\boldsymbol{\mathcal{L}})$, split any collisions in $\boldsymbol{\mathcal{L}}$ that meets the *Split rule*.

C) Update the collaborator list of each node.

Untill The partition converges to a stable statute, that is, no player has an incentive to deviate from its current coalition.

Stage III: Cooperative Secure Transmission

The collision $\boldsymbol{\mathcal{S}}^\star$ that provides the highest utility, which achieves the best secrecy performance at the lowest cost, will be chosen for data transmission.

As defined in (17), the proposed scheme mainly concerns whether the secrecy gain compensates for the reward payed to simulate players into the coalition. Therefore, in this work, we use the individual value order, i.e., the *Pareto order*, to check which partition is more desirable. The coalitions are dynamically formed via an iterative merge-and-split operations:

- *Merge Rule:* Merge any disjoint collections $\{\mathcal{S}_1, \mathcal{S}_2, ...\mathcal{S}_l\}$ whenever $\bigcup_{i=1}^{l} \mathcal{S}_i \succ \{\mathcal{S}_1, \mathcal{S}_2, ...\mathcal{S}_l\}$, that is, small coalitions desire to merge into a larger coalition if merging yields a superior partition on $\mathcal{R}$.
- *Split Rule:* Split any collection $\bigcup_{i=1}^{l} \mathcal{S}_i$ whenever $\{\mathcal{S}_1, \mathcal{S}_2, ...\mathcal{S}_l\} \succ \bigcup_{i=1}^{l} \mathcal{S}_i$, thus, a larger coalition desires to split into multiple disjoint collections if splitting yields a superior partition on $\mathcal{R}$.

According to the above rules, the WFRFT-based PHY-layer security coalitional game can be solved through a three-stage algorithm, given in Algorithm 2. Details are elaborated as follows:

- *Initial Stage:* The source S broadcasts its information to nearby nodes. Following (9), an initial set $\boldsymbol{\mathcal{R}}$, consisting of L suitable nodes, is selected and we assume all suitable nodes in $\boldsymbol{\mathcal{R}}$ are non-cooperative in the beginning. As a result, the partition structure is initialized as $\boldsymbol{\mathcal{L}} := \{\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, ...\boldsymbol{\mathcal{S}}_L\}$, where $\boldsymbol{\mathcal{S}}_i$ $(i = 1, 2, ...L)$ includes one intermediate node only.
- *Coalition Forming Stage:* The partition structure is adjusted adaptively based on the iterative merge-and-split rules. Each individual player in $\boldsymbol{\mathcal{R}}$ first checks the over-

all network status for potential cooperators in vicinity. Then, the Max-Pareto order based iterative merge-and-split operations continues until a stable partition structure is reached. Particularly, the merge (or split) operation is valid if the two following conditions are satisfied: *1)* all the other players in the coalition believe that their individual payoffs can be improved when at least one player is absorbed into (or removed from) the coalition; and *2)* one or more players believe that they can achieve more benefits when being (or not being) a member of the coalition.

- *Cooperative Transmission Stage:* After the stable partition structure is reached, each coalition in the collection reports its individual utility, i.e. the coalition value given by (17). The specific coalition that provides the optimal performance will be chosen for secure date transmission. Note that, if no coalition in the ultimate partition structure can meet the source's secrecy demand, no transmission is allowed by any of the players (intermediate nodes). Under this scenario, the solution for the WFRFT-based coalitional game is $\emptyset$, and no secure communication link is available from S to D.

C. Stability analysis

With the proposed algorithm, a network partition structure consisting of multiple disjoint collisions is obtained. We now analyze the stability of the resulting network structure. The concept of *Nash-stable* is used to evaluate the obtained network structure.

Definition 8: A partition structure $\boldsymbol{\mathcal{L}} := \{\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, ...\boldsymbol{\mathcal{S}}_L\}$ is *Nash-stable* iff $\forall R_i \in \boldsymbol{\mathcal{R}}$, $\boldsymbol{\mathcal{L}} \succ \boldsymbol{\mathcal{L}}'$, where $\boldsymbol{\mathcal{L}}' := \{\boldsymbol{\mathcal{S}}_1, \boldsymbol{\mathcal{S}}_2, ..., \{\boldsymbol{\mathcal{S}}_i - R_i\}, ..., \{\boldsymbol{\mathcal{S}}_j \cup R_i\}, ..., \boldsymbol{\mathcal{S}}_L\}$; and $\boldsymbol{\mathcal{S}}_i \neq \boldsymbol{\mathcal{S}}_j$ [38].

A partition structure is stable in the sense that no player R_i in the game has an incentive to leave its current coalition $\boldsymbol{\mathcal{S}}_i$ to any other coalitions $\boldsymbol{\mathcal{S}}_j$. Furthermore, according to Definition 8, a stable partition implies that no player R_i in current partition structure would be beneficial by joining another coalition while convincing other players that their utilities would not be reduced, i.e.:

$$\begin{aligned} & \nexists R_i \in \boldsymbol{\mathcal{S}}_i; \phi_i(\boldsymbol{\mathcal{S}}_i) > \phi_i(\{\boldsymbol{\mathcal{S}}_j \cup R_i\}) \\ s.t. \quad & \forall R_j \in \boldsymbol{\mathcal{S}}_i; R_j \neq R_i, \phi_j(\boldsymbol{\mathcal{S}}_i) \geq \phi_j(\{\boldsymbol{\mathcal{S}}_i - R_i\}), \\ & \text{and } \forall R_j \in \boldsymbol{\mathcal{S}}_j, \phi_j(\boldsymbol{\mathcal{S}}_j) \geq \phi_j(\{\boldsymbol{\mathcal{S}}_j \cup R_i\}). \end{aligned} \tag{22}$$

Proposition 3: For the WFRFT-based PHY-layer security coalitional game, the proposed Algorithm 2 converges to a *Nash-stable* coalitional structure $\boldsymbol{\mathcal{L}}^\star$.

Proof: We can prove it based on the *Merge and Split Rule*. According to the definition of *Pareto order*, any intermediate node $R_i \in \boldsymbol{\mathcal{R}}$ is able to join any coalition only if none of the original nodes in that coalition could be adversely affected. Start with an arbitrary coalitional structure $\boldsymbol{\mathcal{L}}$, if there exists any node R_i that prefers to switch to another coalition, i.e.$\{\{\boldsymbol{\mathcal{S}}_i - R_i\}, \{\boldsymbol{\mathcal{S}}_j \cup R_i\}, \{\boldsymbol{\mathcal{S}}_l\}_{l \neq i,j}\} \succ \{\boldsymbol{\mathcal{S}}_i, \boldsymbol{\mathcal{S}}_j, \{\boldsymbol{\mathcal{S}}_l\}_{l \neq i,j}\}$, then the current structure $\boldsymbol{\mathcal{L}}$ is not stable. As a consequence, node R_i will be moved from $\boldsymbol{\mathcal{S}}_i$ to $\boldsymbol{\mathcal{S}}_j$ via an iterative merge-and-split operations (i.e., line 15-19 of Algorithm 2).

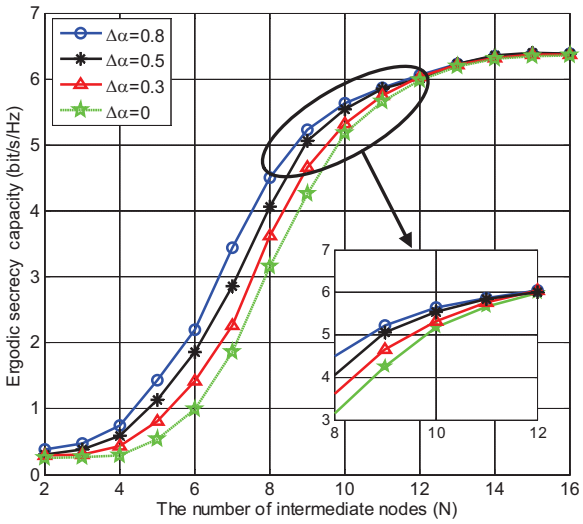


Fig. 2. The secrecy performance of WFRFT-based cooperative system versus number of intermediate nodes in the case of the eavesdropper gaining the full knowledge of WFRFT.

The iterative merge-and-split operations stops until each node satisfies with its current situation. In other words, no one has an incentive to leave its current coalition. As a result, an *Nash-stable* coalitional structure $\boldsymbol{\mathcal{L}}^\star$ will be formed. ■

VI. Simulation Results and Discussions

In this section, simulation results are provided to evaluate the performance of the WFRFT-based PHY-layer security cooperation scheme. The network is set up as follows. The source is located at the origin of a 2.5Km × 2.5Km square with the destination, eavesdropper, and intermediate users randomly deployed in the region. We consider a block quasi-static fading channel modeled by $h_{i,k} = e^{j\phi_{i,k}}\sqrt{\kappa/d_{i,k}^{\mu}}$ with μ the propagation loss exponent, κ the path loss constant, $d_{i,k}$ and $\phi_{i,k}$ the Euclidean distance and the phase offset between terminals i and k, respectively. Particularly, the propagation loss μ is set as 3 and the path loss constant κ is fixed at 1 during the simulation. Moreover, the maximum transmit power of each intermediate node is set to 20 mW, and the noise variance is set to -70 dBm. Without loss of generality, we set parameter $\xi_i \in [0, 1]$ and $\eta = 1$. 20000 independent trials with randomly generated network scenarios are performed to obtain the average results.

We first evaluate the optimality of using WFRFT for PHY-layer security. Fig. 2 shows the secrecy performance of the proposed approach versus the number of intermediate nodes under the scenario where the eavesdropper gains the full knowledge of WFRFT. In particular, $\Delta\alpha = \beta - \alpha$, where β and α represents the WFRFT parameters utilized by the eavesdropper and destination, respectively. Unlike other existing literature where the secrecy of the parameter α directly affects the transmission security [39], Fig. 2 shows that in our proposed scheme secure transmission can still be guaranteed even if the eavesdropper's receiver operates identically with that of the destination. More specifically, when N is small, there exists a slight difference in secrecy performance as $\Delta\alpha$ varies.

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.2017.2712158, IEEE Transactions on Wireless Communications

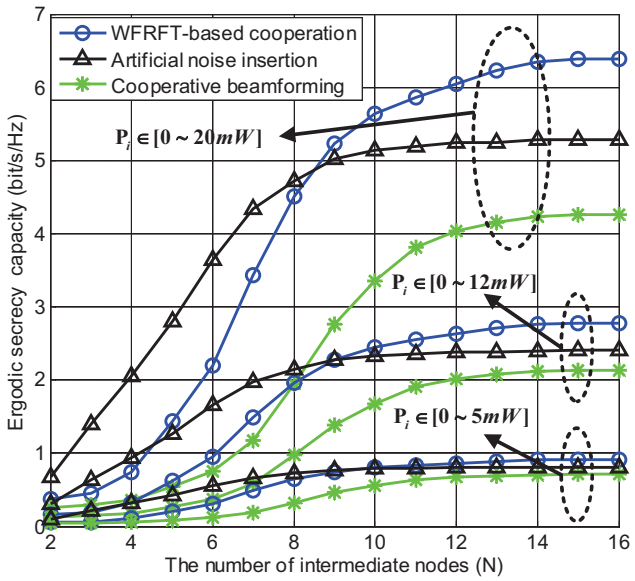


Fig. 3. The secrecy performance versus the available transmission power for WFRFT-based cooperation, beamforming and artificial noise systems.

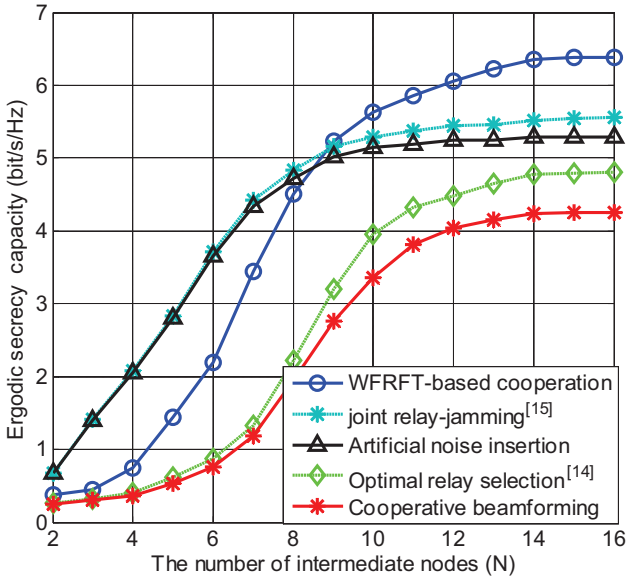


Fig. 4. Secrecy performance comparison of the proposed scheme with artificial noise, beamforming, optimal relay selection and joint relay-jamming schemes.

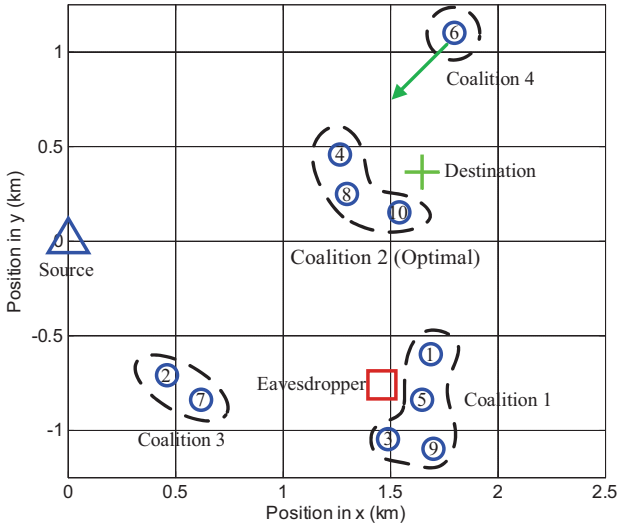


Fig. 5. One snapshot of the final network structure resulting from the proposed coalitional game with $N = 10$ randomly deployed intermediate nodes.

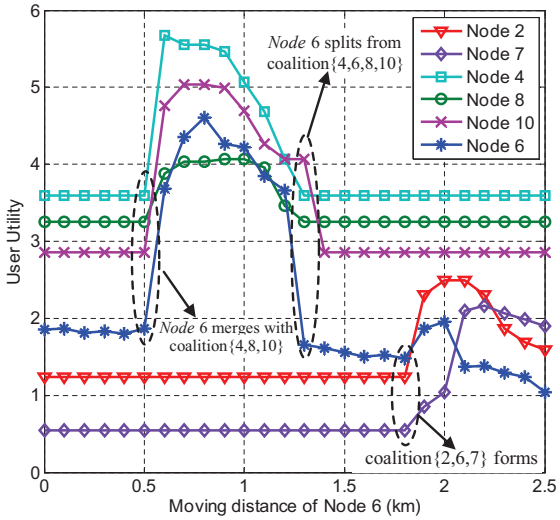


Fig. 6. Self-adaption of Algorithm 2 in handling the mobility of network's topology as Node 6 moves towards Node 2.

However, as N increases, the gap between different curves becomes negligible. The reason is that, with the network scale enlarged, the number of "qualified helper" increases. As a result, the message energy is allocated onto more sub-signals that will selectively degrade the eavesdropper's reception due to the uncertainty of wireless channels, leading to secrecy performance enhancement.

Fig. 3 shows the secrecy performance versus the available transmission power for WFRFT-based cooperation, beamforming and artificial noise schemes. It can be seen that the attainable ergodic secrecy capacity of these three schemes all increase proportionately with the achievable transmission power of intermediate nodes. However, as the achievable transmission power increases, WFRFT-based cooperation scheme outperforms both beamforming and artificial noise schemes. This is because the secrecy of the WFRFT-based cooperation scheme comes from the mutual-interference between the signal components from different intermediate nodes. Therefore, with more achievable transmission power, the intermediate nodes bear more information exchange with D. However, the eavesdropper could not benefit from the increment of the intermediate nodes' power consumption. As a result, the intermediate nodes can provide better chance to form WFRFT-based cooperation with improved secrecy capacity.

In Fig. 4, we compare the WFRFT-based cooperation scheme with beamforming, artificial noise, optimal relay selection and joint relay-jamming schemes, in terms of the secrecy performance. It can be seen that, as the network size

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.2017.2712158, IEEE Transactions on Wireless Communications

N increases, the WFRFT-based cooperative system provides significant secrecy rate gains, reaching up to 121.6% and 149.5% at $N = 14$, compared with the artificial noise and beamforming schemes, respectively. Note that artificial noise scheme outperforms the proposed scheme at the beginning. This due to the fact that, under the small network scale scenario, there is less freedom for the WFRFT-based scheme and beamforming scheme to optimize their transmission strategies. As a result, the artificial noise scheme achieves a better secrecy performance. However, as more intermediate nodes are deployed, the likelihood of finding an optimal coalition with improved secrecy for the WFRFT-based cooperation scheme increases. Besides, it is noticed that both beamforming and artificial noise insertion used in Fig. 4 have been formed as the coalition game. Therefore, a simplified relay selection procedure have already been involved. That's why they exhibit the similar secrecy tendency as the optimal relay selection and joint relay-jamming schemes. More importantly, the secrecy of the WFRFT-based cooperation scheme relies on the mutual-interference between the signal components from different intermediate nodes. Therefore, the WFRFT-based cooperation scheme outperforms the artificial noise scheme since no extra power consumption is required to generate non-information bearing signal.

Next, we evaluate the feasibility of the proposed coalitional game strategy. We start with a simple case consisting of $N = 10$ randomly deployed intermediate nodes. Fig. 5 shows one snapshot of the network structure obtained from the proposed coalitional game. 4 independent coalitions are have been formed in the depicted network. In particular, the coalition formation process follows the iterative merge-and-split rule given by Algorithm 2. For example, node 6, located far away from any other nodes, can not find suitable partners for cooperation. Coalition $\{1,3,5,9\}$ is formed due to the fact that the individual utility $V(\{1,5,3,9\}) = [0.37, 0.61, 0.26, 1.03]$ which is an apparent improvement compared with the zero utilities obtained by acting alone (in the proximity of eavesdropper). Moreover, the coalition $\{4,8,10\}$ is selected as the output for its optimal performance. In general, Fig. 5 illustrates how the distributed intermediate nodes self-organize into multiple disjoint coalitions using Algorithm 2, to improve the PHY-layer secrecy of the network.

Fig. 6 shows the performance of Algorithm 2, considering the node mobility in the network. It shows the individual utilities of nodes $\{2,4,6,7,8,10\}$ as node 6 moves towards node 2 for 2.5 km. As shown in Fig. 5, when node 6 moves towards node 2, it gets closer to D, and hence, its utility increases at first. Meanwhile, the utilities of other nodes remain unchanged as long as node 6's moving distance is less than 0.4 km, since no alteration is made to the network topology. After that, node 6 is absorbed as a new member of collision $\{4,8,10\}$, and the utilities of all four nodes increases significantly. This is because the new collision improves secrecy performance with lower power cost. Further, when the movement distance of node 6 reaches 0.8 km, it begins to move away from its current patenters and the cost in coalition $\{4,6,8,10\}$ increases. As a result, at 1.3 km, node 6 will split from coalition $\{4,7,8,10\}$ to guarantee the performance of the network. When node 6 moves around 1.8 km, it would be beneficial for node 6 to join collision $\{2,7\}$, however, collision $\{4,8,10\}$ will still be the final option due to its superior performance. These results illustrates how the network topology is dynamically self-organized using Algorithm 2.

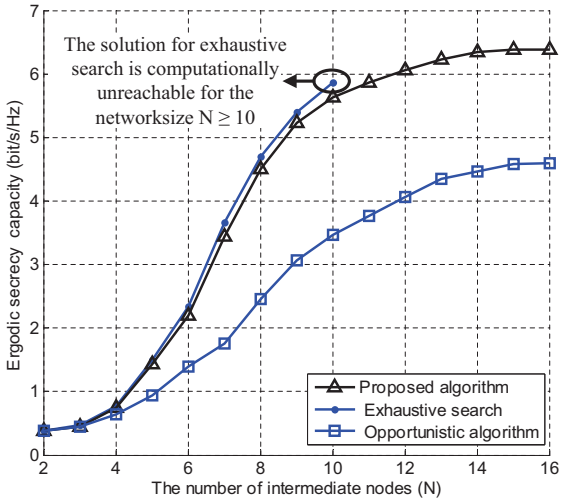


Fig. 7. Performance comparison in terms of secrecy ergodic capacity between Algorithm 2, opportunistic selection and exhaustive searching.

Fig. 7 compares different selection schemes, in terms of secrecy ergodic capacity, with respect to the network size N. It can be seen the proposed coalitional game scheme achieves better secrecy performance, compared with the opportunistic method [22]. The performance gain increases with the network size N. However, there is a performance gap between the optimal exhaustive search solution. This is because that the proposed coalitional game is solved by the distributed merge-and-split algorithm that only provides locally optimal solutions within the discovering range of a collision. Nevertheless, compared to the exhaustive search solution, the proposed algorithm still achieves a comparable performance with a secrecy degradation less than 5% at $N = 10$. Moreover, albeit the performance loss, the proposed algorithm provides a more feasible solution in handling the user cooperation. Particularly, for the network size $N \geq 10$, finding the optimal collisions by exhaustive searching will be computationally infeasible.

VII. Conclusion

In this paper, we have proposed a WFRFT-based cooperation scheme to enhance PHY-layer security in an energy-efficient way. Different from conventional *"artificial noise"* schemes that requires extra jamming signals to disrupt the eavesdroppers reception, based on WFRFT, the proposed scheme can create an identical *"artificial noise"* effect with the information bearing signal to confound the eavesdropper while imposing no impact on the legitimate receiver. To maximize the secrecy of the network efficiently, we have proposed a WFRFT-based PHY-layer security cooperation scheme based on NTU coalitional game and developed a distributed merge-and-split algorithm to autonomously construct the coalition. The proposed algorithm is stable and can efficiently adapt

to dynamic network structure change, such as the mobility of intermediate nodes. Simulation results demonstrate that the WFRFT-based user cooperation scheme can achieve significant performance advantage, in terms of secrecy ergodic capacity, compared with conventional PHY-layer security-oriented user cooperation schemes, such as relay-jamming and cluster-beamforming.

For the future work, we will consider a more general case with the multiple source-destination pairs. In addition, we will also consider how to perform cooperation for PHY layer security without CSI [40, 41].

APPENDIX A
PROOF OF THE PROPERTIES OF CWFRFT

A. Proof of Property 1

Let $a \in \mathbb{R}, b \in \mathbb{R}$ and $a \neq b$. Following the definition of CWFRFT in (3), if $\mathscr{F}_c^a(\mathbf{X}) = \mathscr{F}_c^b(\mathbf{X})$, there must be $\{w_p^a = w_p^b\}_{p=0}^3$, i.e.

$$\sum_{k=0}^{3} \exp\left\{\frac{-2\pi j(a-p)k}{4}\right\} \equiv \sum_{k=0}^{3} \exp\left\{\frac{-2\pi j(b-p)k}{4}\right\} \quad for \quad p = 0,1,2,3. \tag{23}$$

then, the equality of (23) holds when

$$\left(\exp\left(\frac{-2\pi jak}{4}\right) - \exp\left(\frac{-2\pi jbk}{4}\right)\right)_{k=0}^{3} = 0 \tag{24}$$

Therefore, $a - b = 4n, n \in \mathbb{Z}$. ■

B. Proof of Property 2

According to the Periodicity property of CWFRFT, $\mathscr{F}_c^{\alpha+4}(\mathbf{X}) = \mathscr{F}_c^{\alpha}(\mathbf{X})$, Property 2 can be proved if

$$\mathscr{F}_c^{\langle\alpha\rangle_4}(\mathbf{X}) = \boldsymbol{F}^{\langle\alpha\rangle_4} \cdot \mathbf{X}, \tag{25}$$

where $\langle\cdot\rangle_4$ the denotes modulo-4 calculation. Let $\{\alpha, l\} \in \{0,1,2,3\}$, it is easy to verify that

$$w_l^{\alpha} = \begin{cases} 1 & (l = \alpha) \\ 0 & (l \neq \alpha). \end{cases} \tag{26}$$

It is certain that $\mathscr{F}_c^{\alpha}(\mathbf{X}) = \boldsymbol{F}^{\alpha} \cdot \mathbf{X}$, for $\alpha \in \{0,1,2,3\}$. Thus we complete the proof. ■

C. Proof of Property 3

Straightforwardly, Property 3 can be proved if the coefficients of $\mathscr{F}_c^{a+b}(\cdot)$, $\mathscr{F}_c^{a}(\mathscr{F}_c^{b}(\cdot))$ and $\mathscr{F}_c^{b}(\mathscr{F}_c^{a}(\cdot))$ are equivalent, namely, all of the following equations are satisfied.

$$\begin{cases} w_0^{a+b} = w_0^a w_0^b + w_1^a w_3^b + w_2^a w_2^b + w_3^a w_1^b \\ w_1^{a+b} = w_0^a w_1^b + w_1^a w_0^b + w_2^a w_3^b + w_3^a w_2^b \\ w_2^{a+b} = w_0^a w_2^b + w_1^a w_1^b + w_2^a w_0^b + w_3^a w_3^b \\ w_3^{a+b} = w_0^a w_3^b + w_1^a w_2^b + w_2^a w_1^b + w_3^a w_0^b \end{cases} \tag{27}$$

The equality of (27) can be easily verified through some basic algebraic manipulations. ■

APPENDIX B
PROOF OF THEOREM 2

Theorem 2 is proved by induction. For briefness, we use $\{A_{k,l}(\alpha_k)\}_{l=0}^{k-1}$ to denote the weighting coefficients of k-WFRFT.

Step 1 : (Base case) We prove that Theorem 2 holds for $M = 5$, i.e. $\alpha_5 = \frac{5}{4}\alpha_4$, when $\mathbf{W}_4^{\alpha_4} = \mathbf{W}_5^{\alpha_5}$.

By (1) and Theorem 1, we have

$$\mathbf{W}_4^{\alpha_4} = \sum_{n=0}^{3} A_{4,n}(\alpha_4)\boldsymbol{F}^n, \tag{28}$$

and

$$\begin{aligned} \mathbf{W}_5^{\alpha_5} &= \sum_{l=0}^{4} A_{5,l}(\alpha_5)\mathbf{W}_4^{\frac{4l}{5}} \\ &= \sum_{l=0}^{4} A_{5,l}(\alpha_5) \sum_{n=0}^{3} A_{4,n}(\frac{4l}{5})\boldsymbol{F}^n. \end{aligned} \tag{29}$$

Let $\Phi_n = \sum_{l=0}^{4} A_{5,l}(\alpha_5)A_{4,n}(\frac{4l}{5})$, then we have $\mathbf{W}_5^{\alpha_5} = \sum_{n=0}^{3}\Phi_n\boldsymbol{F}^n$. Explicitly, $\mathbf{W}_5^{\alpha_5} = \mathbf{W}_4^{\alpha_4}$ iff $\Phi_n = A_{4,n}(\alpha_4)$, by which the relationship between α_4 and α_5 can be proved.

When $n = 0$***:*** Let $\Delta_l = A_{5,l}(\alpha_5)A_{4,0}(\frac{4l}{5})$, where $l = 0,1,2,3$. According to *Property 2*, we have $A_{4,0}(0) = 1$, and therefore

$$\Delta_0 = A_{5,0}(\alpha_5) = \frac{1}{5}\frac{1-\exp\left[-2\pi j(\alpha_5)\right]}{1-\exp\left[-2\pi j(\alpha_5)/5\right]}. \tag{30}$$

By (2), the following equation holds

$$\sum_{l=1}^{4}\Delta_l = \frac{1 - 5\exp\left(-8\pi j\alpha_5/5\right) + 4\exp\left(-2\pi j\alpha_5/5\right)}{20[1-\exp\left(-2\pi j\alpha_5/5\right)]} \tag{31}$$

Substituting (30) and (31) into (29) yields:

$$\Phi_0 = \frac{1-\exp\left(-8\pi j\alpha_5/5\right)}{4[1-\exp\left(-2\pi j\alpha_5/5\right)]}. \tag{32}$$

Moreover, since

$$A_{4,0}(\alpha_4) = \frac{1-\exp\left(-2\pi j\alpha_4\right)}{4[1-\exp\left(-2\pi j\alpha_4/4\right)]},$$

it holds that if $A_{4,0}(\alpha_4) = \Phi_0$, there must be $\alpha_5 = \frac{5}{4}\alpha_4$.

The same results can also be obtained for the scenarios $n = 1, 2$ and 3, and the proof is omitted here.

Step 2: (Inductive step) Suppose that Theorem 2 holds for $M = k$ $(k > 5)$. i.e., if $\mathbf{W}_4^{\alpha_4} = \mathbf{W}_k^{\alpha_k}$, there must be $\alpha_k = \frac{k}{4}\alpha_4$. Then, based on this assumption, we prove that Theorem 2 holds for $M = k+1$ $(k > 5)$.

To prove the relationship between α_k and α_4, we first prove that $\alpha_{k+1} = \frac{k+1}{k}\alpha_k$ is true for $\mathbf{W}_k^{\alpha_k} = \mathbf{W}_{k+1}^{\alpha_{k+1}}$. According to (1), $\mathbf{W}_{k+1}^{\alpha_{k+1}}$ can be expressed by

$$\mathbf{W}_{k+1}^{\alpha_{k+1}} = \sum_{l=0}^{k} A_{k+1,l}(\alpha_{k+1})\mathbf{W}_4^{\frac{4l}{k+1}}. \tag{33}$$

With the aforementioned assumption, by substituting $\mathbf{W}_4^{\alpha_4}$ with $\mathbf{W}_k^{\alpha_k}$, (33) can be rewritten as:

$$\mathbf{W}_{k+1}^{\alpha_{k+1}} = \sum_{l=0}^{4} A_{k+1,l}(\alpha_{k+1})\mathbf{W}_k^{\frac{kl}{k+1}} \tag{34}$$

Since $\alpha_{k+1} = \frac{k+1}{k}\alpha_k$, using (1), we obtain the following constraint:

$$\sum_{l=0}^{k} A_{k+1,l}(\alpha_{k+1}) \sum_{n=0}^{k-1} A_{k,n}(\frac{kn}{k+1})\mathbf{T}^{\frac{4n}{k}} = \sum_{n=0}^{k-1} A_{k,n}(\alpha_k)\mathbf{T}^{\frac{4n}{k}} \quad (35)$$

Denote $\Phi_n = \sum_{l=0}^{k} A_{k+1,l}(\alpha_{k+1})A_{k,n}(\frac{kn}{k+1})$. Then, the equality of (35) holds iff $\Phi_n = A_{k,n}(\alpha_k)$.

Similar to *Step 1*, we consider the scenario $n = 0$ for example. Denote $\Delta_l = A_{k+1,l}(\alpha_{k+1})A_{k,n}(\frac{kn}{k+1})$. When $n = 0$, $A_{k,0}(0) = 1$, we have :

$$\Delta_0 = A_{k+1,l}(\alpha_{k+1}) = \frac{1}{k+1}\frac{1-\exp\left[-2\pi j\alpha_{k+1}\right]}{1-\exp\left[\frac{-2\pi j\alpha_{k+1}}{k+1}\right]}. \quad (36)$$

whereas for $\{\Delta_l\}_{l=1}^{k}$, it holds that

$$\sum_{l=1}^{k}\Delta_l = \frac{1-(k+1)\exp\left(\frac{-2\pi kj\alpha_{k+1}}{k+1}\right)+k\exp\left(-2\pi j\alpha_{k+1}\right)}{k(k+1)\left[1-\exp\left(\frac{-2\pi j\alpha_{k+1}}{k+1}\right)\right]} \quad (37)$$

With (36) and (37), we obtain:

$$\Phi_0 = \frac{1-\exp\left(\frac{-2\pi kj\alpha_{k+1}}{k+1}\right)}{k\left[1-\exp\left(\frac{-2\pi j\alpha_{k+1}}{k+1}\right)\right]}. \quad (38)$$

According to the constraint $\Phi_0 = A_{k,0}(\alpha_k)$, the following equation holds:

$$\frac{1-\exp\left(\frac{-2\pi kj\alpha_{k+1}}{k+1}\right)}{k\left[1-\exp\left(\frac{-2\pi j\alpha_{k+1}}{k+1}\right)\right]} = \frac{1-\exp\left[-2\pi j\alpha_k\right]}{k\left[1-\exp\left(\frac{-2\pi j\alpha_k}{k}\right)\right]}. \quad (39)$$

Therefore, it is true that $\alpha_{k+1} = \frac{k+1}{k}\alpha_k$. Then, by substituting α_k with $\frac{k}{4}\alpha_4$, we obtain that $\alpha_{k+1} = \frac{k+1}{4}\alpha_4$.

Thus, we complete the proof. ■

APPENDIX C
PROOF OF THEOREM 3

Theorem 3 is proved by contradiction. Suppose that the equality of $\mathbf{W}_M^{\alpha}\cdot\mathbf{W}_M^{\beta} = \boldsymbol{I}$ holds under the assumption $\alpha+\beta \neq 0$ or $\{A_l(\alpha)\}_{l=0}^{M-1}$ (or/and $\{A_l(\beta)\}_{l=0}^{M-1}$) are contaminated. Typically, $\{A_l(\alpha)\}_{l=0}^{M-1}$ is contaminated, implying that the weighting coefficients are not generated properly, i.e.:

$$A_l(\alpha) = \frac{1}{M}\frac{1-\exp\left[-2\pi j(\alpha-l)\right]}{1-\exp\left[-2\pi j(\alpha-l)/M\right]} + \Delta_l. \quad (40)$$

The proof can be completed by considering the following two cases.

Case 1: Suppose that $\alpha+\beta = \eta$. According to the *addition axiom* given in Definition 2, it holds that $\mathbf{W}_M^{\alpha}\cdot\mathbf{W}_M^{\beta} = \mathbf{W}_M^{\eta} = \boldsymbol{I}$, which contradicts the *boundary axiom.*

Case 2: Suppose that

$$\begin{aligned} A_l(\alpha) &= \frac{1}{M}\frac{1-\exp\left[-2\pi j(\alpha-l)\right]}{1-\exp\left[-2\pi j(\alpha-l)/M\right]} + \Delta_l, \\ A_l(\beta) &= \frac{1}{M}\frac{1-\exp\left[-2\pi j(\beta-l)\right]}{1-\exp\left[-2\pi j(\beta-l)/M\right]}, \end{aligned} \quad (41)$$

which means that only $\{A_l(\alpha)\}_{l=0}^{M-1}$ is contaminated.

For briefness, we only consider the case where $M = 4$ (similar results can also be obtained for $M \neq 4$). According to the *addition axiom*, we have $\mathbf{W}_4^{\alpha}\cdot\mathbf{W}_4^{\beta} = \mathbf{W}_4^{\alpha+\beta}$. Since $\mathbf{W}_4^{\alpha+\beta} = \sum_{n=0}^{3} A_l(\alpha+\beta)\boldsymbol{F}^n$, it holds that $\mathbf{W}_4^{\alpha+\beta} = \boldsymbol{I}$, when $A_0(\alpha+\beta) = 1$ and $\{A_l(\alpha+\beta) = 0\}_{l=1}^{3} = 0$. Substituting $A_l(\alpha)$ and $A_l(\beta)$ into (27), when $\alpha+\beta = 0$, we have:

$$\begin{cases} A_0(0) = 1 + \sum_{l=0}^{3}\Delta_l A_{\langle 4-l\rangle_4}(\beta) = 1 \\ A_1(0) = 0 + \sum_{l=0}^{3}\Delta_l A_{\langle 5-l\rangle_4}(\beta) = 0 \\ A_2(0) = 0 + \sum_{l=0}^{3}\Delta_l A_{\langle 6-l\rangle_4}(\beta) = 0 \\ A_3(0) = 0 + \sum_{l=0}^{3}\Delta_l A_{\langle 3-l\rangle_4}(\beta) = 0 \end{cases} \quad (42)$$

Then, the equality of (42) is achieved when $\{\Delta_l = 0\}_{l=0}^{3}$, which contradicts the assumption.

Similarly, we can obtain the same results for the scenarios that only $\{A_l(\beta)\}_{l=0}^{M-1}$ is contaminated or both $\{A_l(\alpha)\}_{l=0}^{M-1}$ and $\{A_l(\beta)\}_{l=0}^{M-1}$ are contaminated. Thereby, we conclude that the constraints in Theorem 3 must be true to achieve $\mathbf{W}_M^{\alpha}\mathbf{W}_M^{\beta} = \boldsymbol{I}$, and thus the proof is complete.

ACKNOWLEDGMENT

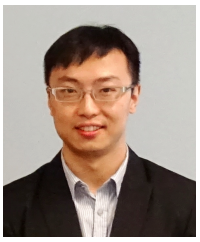
This work was completed during Xiaojie Fang's visit to the Broadband Communications Research Group (BBCR), University of Waterloo and was supported by the National Basic Research Program of China under Grant 2013CB329003, the National Nature Science Foundation of China under Grant 61671179 and the Natural Sciences and Engineering Research Council (NSERC) of Canada.

REFERENCES

[1] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: challenges and solutions," *IEEE Wireless Commun.*, vol. 21, no. 1, pp. 33–41, Feb. 2014.
[2] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.
[3] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for crns," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.
[4] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wirel. Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[6] A. D. Wyner, "The wiretap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, May. 1975.
[7] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Info. Theory*, 2006, pp. 356–360.
[9] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wirel. Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.
[10] X. He, A. Khisti, and A. Yener, "Mimo broadcast channel with arbitrarily varying eavesdropper channel: Secrecy degrees of freedom," in *Proc. of IEEE GLOBECOM'11*, 2011.
[11] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[12] R. F. Schaefer and S. Loyka, "The secrecy capacity of compound gaussian mimo wiretap channels," *IEEE Trans. Inform. Theory*, vol. 61, no. 10, pp. 5535–5552, Oct 2015.
[13] 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. 3532–3545, Jul. 2012.

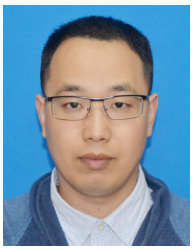
[14] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[15] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.
[16] R. Negi and S. Goel, "Secret communication using artificial noise," in *Vehicular Technology Conference (VTC)*, Sep. 2005.
[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[18] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, 2012.
[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct 2010.
[20] 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, Mar. 2010.
[21] 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," *Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.
[22] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.
[23] T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov 2015.
[24] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, June 2015.
[25] L. Mei, X. Sha, and N. Zhang, "The approach to carrier scheme convergence based on 4-weighted fractional fourier transform," *IEEE Commun. Lett.*, vol. 14, no. 6, pp. 503–505, Jun. 2010.
[26] K. Wang, X. Sha, L. Mei, and X. Qiu, "Performance analysis of hybrid carrier system with mmse equalization over doubly-dispersive channels," *IEEE Commun. Lett.*, vol. 16, no. 7, pp. 1048–1051, Jul. 2012.
[27] Y. Li, X. Sha, F.-C. Zheng, and K. Wang, "Low complexity equalization of hcm systems with dpfft demodulation over doubly-selective channels," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 862–865, Jul. 2014.
[28] L. Mei, Q. Zhang, X. Sha, and N. Zhang, "WFRFT precoding for narrowband interference suppression in DFT-based transmission systems," *IEEE Commun. Lett.*, vol. 17, no. 10, pp. 1916–1919, Oct. 2013.
[29] K. Wang, X. Sha, and Y. Li, "Iterative frequency-domain equalization for wfrft and est based modulation schemes over doubly selective wireless fading channels," in *Proceedings of Personal Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2013.
[30] Z. Wang, L. Mei, X. Wang, X. Sha, and N. Zhang, "Ber analysis of hybrid carrier system based on wfrft with carrier frequency offset," *Electronics Letters*, vol. 51, no. 21, pp. 1708–1709, Oct. 2015.
[31] Q. Ran, D. S. Yeung, E. C. C. Tsang, and Q. Wang, "General multifractional fourier transform method based on the generalized permutation matrix group," *IEEE Trans. Signal Process.*, vol. 53, no. 1, pp. 83–98, Jan. 2005.
[32] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game:interaction between source, eavesdropper, and friendly jammer," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–11, 2010.
[33] 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. Inf. Forensics Sec.*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
[34] X. Fang, X. Wu, N. Zhang, X. Sha, and X. Shen, "Safeguarding physical layer security using weighted fractional fourier transform," in *Proc. of IEEE GLOBECOM'16*, Dec 2016.
[35] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Process. Mag.*, vol. 26, no. 5, pp. 77–97, Sep. 2009.
[36] W. Saad, Z. Han, T. Başar, M. Debbah, and A. Hjørungnes, "Distributed coalition formation games for secure wireless transmission", journal="j. mobile netw. appl", year="2011", volume="16", number="2", pages="231–245",."
[37] T. S. Ferguson, "Game theory." [Online]. Available: https: // www.math.ucla.edu/ tom/Game_Theory/mat.pdf
[38] K. Akkarajitsakul, E. Hossain, and D. Niyato, "Coalition-based cooperative packet delivery under uncertainty: A dynamic bayesian coalitional game," *IEEE. Trans. Mob. Comput.*, vol. 12, no. 2, pp. 371–385, Feb. 2013.
[39] X. Fang, X. Sha, and Y. Li, "Secret communication using parallel combinatory spreading wfrft," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 62–65, Jan. 2015.
[40] T. X. Zheng, H. M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for df relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.
[41] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, accepted for publication, 2017. [Online]. Available: http://ieeexplore .ieee.org/stamp/stamp.jsp?tp=&arnumber=7812681&isnumber=5497975

Xiaojie Fang (IEEE S'14) received his B.Sc. and M.Sc. degrees from Department of Electronics and Information Engineering, Harbin Institute of Technology in 2010 and 2012, respectively. He was a visiting scholar in the Broadband Communications Research Group (BBCR), Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is currently pursuing the Ph.D. degree with the Department of Electronics and Information Technology, Harbin Institute of Technology. His current research interests include physical layer security, coding and modulation theory.



Ning Zhang (IEEE S'12-M'16) received the Ph.D degree from University of Waterloo in 2015. He received his B.Sc. degree from Beijing Jiaotong University and the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2010, respectively. From May 2015 to Apr. 2016, he was a postdoc research fellow at BBCR lab in University of Waterloo. Since May 2016, he has been a postdoc research fellow at Wireless Computing lab at University of Toronto. He is now an associate editor of International Journal of Vehicle Information and Communication Systems and a guest editor of Mobile Information System. He is the recipient of the Best Paper Award at IEEE Globecom 2014 and IEEE WCSP 2015. His current research interests include sensor networks, next generation wireless networks, software defined networking, green communication, and physical layer security.

Shan Zhang (IEEE S'13-M'16) received her Ph.D. degree in Department of Electronic Engineering from Tsinghua University and B.S. degree in Department of Information from Beijing Institute Technology, Beijing, China, in 2016 and 2011, respectively. She is currently a post doctoral fellow in Department of Electronical and Computer Engineering, University of Waterloo, Ontario, Canada. Her research interests include resource and traffic management for green communication, intelligent vehicular networking, and software defined networking. Dr. Zhang received the Best Paper Award at the Asia-Pacific Conference on Communication in 2013.



Dajiang Chen (IEEE M'15) is currently a Post Doctoral Fellow at the University of Waterloo, Waterloo, ON, Canada. He is also a Post Doctoral Fellow in the School of information and software Engineering at University of Electronic Science and Technology of China. He received the B.Sc. degree in 2005 and the M.Sc. degree in 2009 from Neijiang Normal University and Sichuan University, respectively, and the Ph.D. degree in information and communication engineering from UESTC in 2014. His current research interest includes Information Theory, Channel coding, and their applications in Wireless Network Security, Wireless Communications and other related areas.

Xuejun Sha (IEEE M'09) is a Professor in Communication Research Center (CRC) at the Department of Electronics and Information Engineering, Harbin, China. He joined CRC as a Teaching Assistant in 1993, and became a Lecturer and a Professor in 1994 and 2000, respectively. He received his Ph.D. degree in Communications and Electronics Systems from Harbin Institute of Technology, in 1995. From 1997 to 1998, he was a postdoctoral fellow in Korea University, Seoul, Korea. His main research interests include communication network, wireless ad-hoc network, and broadband wireless access.

Xuemin (Sherman) Shen (IEEE M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Professor and the Associate Chair for Graduate Studies, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shens research focuses on resource management in wireless networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He was an elected member of IEEE ComSoc Board of Governor, and the Chair of Distinguished Lecturers Selection Committee. Dr. Shen served as the Technical Program Committee Chair/Co-Chair for IEEE Globecom16, Infocom14, IEEE VTC10 Fall, and Globecom07, the Symposia Chair for IEEE ICC10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC08, the General Co-Chair for ACM Mobihoc15, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, IET Communications, and Editor-in-Chief for IEEE Internet of Things Journal; a Founding Area Editor for IEEE Transactions on Wireless Communications; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo, the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002, 2007, 2016 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.