IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 11, 2018, accepted May 28, 2018, date of publication June 1, 2018, date of current version June 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2842826

A Novel Physical Layer Security Scheme in OFDM-Based Cognitive Radio Networks

HURMAT ALI SHAH AND INSOO KOO, (Member, IEEE)
School of Electrical/Electronics and Computer Engineering, University of Ulsan, Ulsan 680-749, South Korea

Corresponding author: Insoo Koo (iskoo@ulsan.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea, Ministry of Education, under Grant 2015R1D1A1A09057077, and in part by the Korean Government (MSIT) under Grant 2018R1A2B6001714.

ABSTRACT In this paper, a physical-layer-security scheme for an underlay relay-based cognitive radio network (CRN) that uses orthogonal frequency-division multiplexing (OFDM) as the medium access technique is proposed. Resource allocation in relay-aided CRNs becomes a hard problem especially if it is under security threat. Different from conventional relay-based OFDM schemes, in the paper, we consider the relay network which has two dedicated relay nodes; one relay which is capable of subcarrier mapping forward the received signal to the destination and the other sends a jamming signal to add noise to the signal received by the eavesdropper. Optimization is performed under a unified framework where power allocation at the source node, power allocation, and subcarrier mapping in the relay network are optimized to maximize the secrecy rate of the CRN while satisfying the maximum transmission power constraints and the interference threshold of the PU. The power allocation problem at the forwarding relaying node is a non-convex optimization problem. Therefore, at first, the optimization problem is simplified and a closed-form solution is obtained which satisfies the maximum PU interference constraint. Afterward, the optimization problem is solved for satisfying the maximum transmission power constraint. An algorithm is also proposed for subcarrier mapping at the forwarding relaying node. The proposed power allocation method and a subcarrier mapping scheme have low complexity, compared with the baseline schemes. Finally, simulation results are provided for different parameters to show the performance improvement of the proposed scheme in terms of secrecy rate.

INDEX TERMS Cognitive radio networks, physical layer security, optimal power allocation, artificial noise, OFDM based cognitive radio network, subcarrier mapping in relay aided OFDM network, power allocation for secrecy rate maximization.

I. INTRODUCTION

Cognitive radio is an answer to the spectrum scarcity problem, which is induced by pervasive use of wireless spectrum for various purposes. In cognitive radio networks, a secondary user, or cognitive radio (CR) user, opportunistically accesses the spectrum occupied by the primary user (PU), provided the PU is inactive or interference with PU communications (caused by CR user communications) is below a specified threshold. The first method for accessing the spectrum is called overlay mode, and the second is called underlay mode. In underlay mode, because of the coexistence of two different kinds of communications, each with different levels of priority, power allocation in CR communications becomes a design issue on which the performance of the whole system depends. Orthogonal frequency division multiplexing (OFDM) has shown great promise in improving transmission efficiency. By minimizing inter-symbol interference, high-speed data transmission is made possible. If the concept of OFDM is integrated into cognitive radio, spectrum utilization will improve. OFDM-based cognitive radio can become an important future-generation wireless system. The key problem in relay-based cognitive radio networks that use OFDM as a spectrum access technique is power allocation on different hops. In a multi-hop network, the channel gain over different hops may be mutually independent for all subcarriers. So, the subcarriers that face deep fading over one hop may not experience deep fading over the other hops [1]. This fact allows a degree of freedom in resource allocation, which allows for properly matching subcarriers on different hops. This is called sub-carrier matching [1]. Compared with

traditional single-hop OFDM systems, resource allocation in a relay-based multi-hop OFDM system becomes more challenging. Resource allocation is made more difficult by the interference constraint in cognitive radio systems. In the context of a cognitive radio network (CRN), a subcarrier with the highest gain over one hop may also cause the most interference with the PU, and mapping this subcarrier to a carrier with the highest gain over the next hop may result in strong interference with the PU.

Wireless communications suffer from security issues where an eavesdropper overhears legitimate communications. Confidentiality of wireless communications is attracting much research interest. Traditionally, the security for communications systems is dealt with at higher layers. But because of the lack of infrastructure in ad-hoc networks, such as a CRN, security at higher layers in ad-hoc networks becomes infeasible. The encryption algorithms used in higher-layer security approaches can be compromised as computational power is becoming increasingly available to users that can be eavesdroppers [2]. This approach is also made complicated by the difficulty with secret key distribution. Thus, physical layer-security techniques have received greater interest of late to ensure security at the physical layer. Physical layer-security approaches exploit properties of the communications channel to ensure secrecy. It is an information-theoretic approach, and secrecy is achieved by using channel codes and signal processing techniques at the physical layer.

Ozarow and Wyner [3] showed that perfectly secure information can be communicated at a nonzero rate from source to destination, while leaving the eavesdropper unable to learn anything about the information being communicated, referred to as secrecy rate. It is defined as the difference between the transmission rate of the source-destination link (which is the legitimate transmission) and the source-eavesdropper link. A simple but efficient way to increase the secrecy rate in communications systems is with the use of artificial noise [4]. The decoding capability of the eavesdropper is degraded by introducing controlled interference into the eavesdropper link. When users in a communication are restricted to having one antenna, then an array of external relays can be employed where some relays forward the received information to the destination and others send a jamming signal against the eavesdropper. The power of the relay that forwards the received information, combined with the jamming power of the relay that functions as a jamming relay node, causes interference with PU communications. In the context of an OFDM-based CRN, providing physical layer security becomes a hard problem. Along with subcarrier mapping over different hops, power allocation at the source, the forwarding relaying node, and the jamming relay node becomes crucial for the secrecy rate of the system under a maximum interference constraint.

Optimal power allocation schemes for minimizing symbol error rates and outage probability, respectively, for a multi-node relay transmission were carried out by Sadek *et al.* [5] and Seddik *et al.* [6]. But these schemes are not applicable in the context of a CRN, as the schemes designed by Sadek *et al.* [5] and Seddik *et al.* [6] may violate the interference constraints that safeguard the communications of primary users. We are investigating physical layer security for an OFDM-based CRN. The transmitter embeds artificial noise in its transmission, which is designed to avoid interference with the legitimate receiver and only harm the eavesdropper [7]–[9]. However, those various schemes [7]–[9] consider multiple antennas, and artificial noise cannot be used in a system where the nodes have only one antenna. In ad-hoc networks and CRNs, the nodes are assumed to be of low complexity with fewer computational resources. So, to provide physical layer security in a CRN, external relays that act as jammers can be employed. This approach is referred to as cooperative jamming.

Zhang *et al.* [10] considered physical layer security in underlay full duplex cognitive radio system while the secrecy performance of full duplex multi-antenna wiretap networks in presence of a jammer was analyzed by [11]. Some other works [12]–[14] have also discussed basic schemes using multiple external relays for cooperative jamming. The optimal design of cooperative jamming relay weights to maximize the secrecy rate was investigated by Zheng *et al.* [15]. A combination of two relays, where one relay forwards the transmitted signal while the other relay acts as a cooperative jammer, was discussed by Krikidis *et al.* [16]. Ding *et al.* [17] combined cooperative jamming with interference alignment. Beamforming for improving secrecy capacity was investigated by Wang *et al.* [18]. The schemes and works discussed here cannot be directly applied to CRNs because of their different contexts. CRNs have special features: (1) the PU always has first priority when using the spectrum in a CRN, and (2) it is unreasonable to assume that the PU always cooperates with CR users unconditionally. Lee *et al.* [19] studied a cooperation-based access strategy that improves the secrecy rate of the primary link but at the cost of employing multiple antennas. A low-complexity but efficient solution needs to be investigated, where a minimum number of relays with a single antenna are employed. Subcarrier assignment and power allocation to subcarriers are the most important parameters on which the capacity and performance of OFDM systems depend. Mu *et al.* [20] studied joint subcarrier assignment and power allocation for decode-and-forward multi-relay OFDM systems. The problem was formulated as joint optimization of three types of resources (subcarrier, power, and relay) and was solved through dividing the optimization problem into subproblems with dual relations. In a study by Ho *et al.* [21] each node was constrained by the maximum power allowed, and a power-allocation scheme was proposed for an OFDM-based two-way relay link. Interference with the PU is the foremost design constraint in a CRN. Jitvanichphaibool *et al.* [22] proposed a scheme that suppresses interference with the primary user by employing multi-antenna relay nodes. Bansal *et al.* [23] studied power allocation in an OFDM-based CRN, and Yan and Wang [24] extended the work to

a relay-aided transmission scenario, and proposed a sub-optimal algorithm that optimizes both source and relay power. Relay assignment also affects the performance of OFDM-based multi-relay systems. Jia *et al.* [25] proposed an optimal strategy for spectrum allocation and relay assignment. As described earlier, a new degree of freedom is allowed for resource allocation in multi-hop OFDM networks as the subcarriers that face deep fading over one hop may not experience deep fading over another hop. The concept of subcarrier-mapping was first introduced by Herdin [26], who showed that system throughput can be enhanced if the subcarriers of two hops are coupled in order of magnitude. Hammerstrom and Wittneben [27] and Li *et al.* [28] considered joint power allocation and subcarrier matching in amplify-and-forward, and decode-and-forward networks, respectively.

In underlay cognitive radios managing the interference caused to legitimate transmissions is of utmost importance. Interference alignment (IA) based strategies are employed to zero-cross the interference caused to the CR receiver. Interference alignment is the concept where multiple interfering signals are consolidated into a small subspace at the receiver so that the number of interference-free dimensions remaining for the desired signal can be maximized [29]. IA is adopted to analyze the precise secure degree of freedom of many kinds of wireless networks based on information theoretic aspect [30]–[32]. Nevertheless the physical layer security aspects of IA-based wireless networks have received very little attention in the literature. Zhao *et al.* [13] studied the systematic analysis of physical layer security of IA-based networks. The concept of artificial noise (AN) can be used together with the idea of IA in low signal to noise ratio (SNR) regimes in underlay cognitive radio networks to improve to increase the secrecy throughput. Introducing AN and aligning the interference caused by the AN can degrade the throughput performance of the wireless networks which is rectified by using the spectrum opportunistically.

As explained earlier, abiding by the interference threshold and the co-existence of CR user and PU on the same spectrum band are hard problems, which become harder when secrecy of the communication is considered. In this paper, we consider physical layer security and formulate a novel physical layer-security scheme for OFDM-based CRNs under maximum interference constraints and total power constraints. Power and subcarrier mapping optimization is carried out to maximize the secrecy rate. An optimal power allocation algorithm is proposed that maximizes the CR system secrecy capacity under maximum interference and power constraints. The interference constraint protects the PU communications from harmful interference, and thus, guarantees co-existence in the same spectrum of both the PU and CR users. The interference constraint can be seen as a way of interference alignment. The interference caused is such that it causes maximum damage to the external eavesdropper's signal while the interference caused by the jamming signal to the legitimate transmissions is managed by aligning the level of power allocated at the forwarding relaying node and the jamming relay node. The maximum power constraint is motivated by the fact that in sensor networks and ad-hoc systems like a CRN, long-term power consumption is a major concern; so, restricting the total transmission power is an effective way to satisfy the long-term power constraint. In our proposed scheme, one relay, known as forwarding relaying node, forwards the source information, and the other, known as jamming relay node, sends a jamming signal against the eavesdropper. On the forwarding relaying node which forwards the source information, subcarrier mapping is also performed so as to reduce the total interference with the PU and to maximize the secrecy rate. Using maximum interference and power constraints, optimal power allocation (PA) is formulated at the forwarding relaying node, which maximizes the CR system secrecy rate. A global solution can not be formed for the PA problem because it is non-convex. So, due to the non-convex nature of the problem the maximum transmission power constraint is not applied at first and is relaxed. After obtaining a closed form solution by solving the simplified PA problem through the Cauchy-Shwartz inequality, the problem is solved for satisfying the maximum transmission power constraint. The final solution is a sub-optimal one but satisfies both the constraints. PA is also performed at the source and at the jamming relay node which satisfy the maximum interference to the PU constraint and the constraint of maximum transmission power at the source node and the jamming relay node.

Beamforming in addition to AN is considered in [33]–[36]. Ng *et al.* [33] have considered a successive refinement scheme (SRC) which is one of the techniques for scalable video coding (SVC). Layered video coding based on SRC is used to encode video information. A beamforming vector is formed for video information in each layer and AN is added for providing communication security in the secondary network. Both the primary transmitter and secondary transmitter are equipped with multiple antennas. The complexity of the scheme proposed in [33] is higher in terms of computational resources but we have considered low complexity CR users in this paper as in practice CR users may not have high computational resources. Beamforming also takes computationally more resources than AN. We have focused on artificial noise through a jamming relay node which has less computational resources but the AN generated is taken into account in the power allocation at the forwarding relay node which makes it a non-trivial problem. The schemes in [34] and [35] proposed simultaneous wireless information and power transfer (SWIPT) for energy harvesting and beamforming is studied for secure information transfer. The cognitive base station (CBS) is equipped with multiple antennas in [34] and the information transfer through beamforming is aided by AN while in [35] Zhou *et al.* have considered AN-aided beamforming in non-orthogonal multiple access (NOMA) mode of spectrum access. The authors in [35] claim that the theoretic information capacity which is achieved by NOMA is higher than orthogonal multiple access (OMA) but

at the cost of increasing the implementation complexity of the receiver. Zhou *et al.* [35] have focused on improving the security of NOMA based CRN using SWIPT while in this work we have focused on improving physical layer security of OFDM-based CRN by formulating non-convex power allocation optimization problem which is solved through integer point method and solving the closed form solution of the simplified problem using Cauchy-Shwartz inequality. In [36] a SWIPT based power minimization problem is formulated by using non-linear energy harvesting model. The primary base station (PBS) also helps the CBS in transmitting AN so the scheme considers cooperation between the PU network and CRN while also considering computationally rich nodes. Our proposed scheme is relay based scheme where the jamming relay node sends AN to the eavesdropper but the effect of the AN is taken into account in the power allocation at the forwarding relay node and thus the power allocated at the forwarding relay node is adjusted according to the AN. We also consider physical layer security for OFDM-based CRN which is not studied exhaustively in literature. The subcarrier mapping at the forwarding relaying node alongwith optimization of power allocation at different nodes is a problem which is not studied before in literature according to the best of our knowledge.

Our proposed scheme seamlessly combine AN with IA. The power allocation scheme at both jamming relay node and the forwarding relaying node takes into consideration the effect of interference caused. The power allocated at source implicitly takes into consideration the interference caused to the PU. The power allocation scheme at the forwarding relaying node takes into consideration the power allocated at the jamming relay node and thus the level of interference which the jamming relay node can cause to the legitimate destination is managed. This can be seen as interference alignment at the forwarding relaying node. The subcarrier mapping done at the forwarding relaying node is meant to reduce leakage of useful information to the eavesdropper. The interference caused by jamming signal is aligned at the forwarding relaying node implicitly and thus the AN generated is made to affect to eavesdropper only.

The rest of this paper is divided as follows. Section II presents the system model and the problem formulation. Section III discusses the problem in detail and presents our proposed solution. Section IV deals with results and analysis of our proposed scheme, while Section V concludes the paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

Section II-A presents our proposed system model, Section II-B presents the constraints on our optimization problem, and Section II-C formulates our given problem.

A. SYSTEM MODEL

We consider a CR system with one CR sender (known as the source), one CR destination, and two relays, as shown in Fig. 1. We assume that the destination is located far outside the transmission range of the source, and thus, cannot directly receive the source communication. A relay network consisting of two relays is proposed. The forwarding relaying node forwards the received signal to the destination, and the jamming relay node, sends a jamming signal to affect the signal received by an eavesdropper. We assume that the forwarding relaying node is a dedicated relay node which has more and computational resources as compared to ad-hoc nodes.

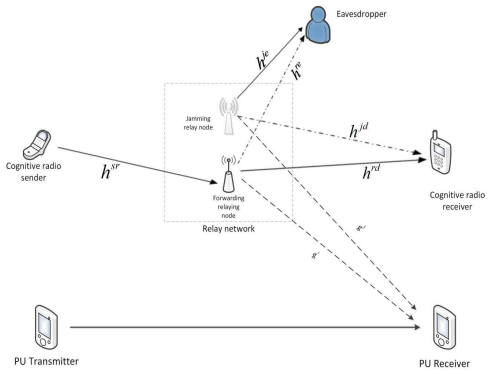

FIGURE 1. The system model.

In the first phase of communication, the source transmits to the relay network. In the second phase, the forwarding relaying node sends the received data using amplify-and-forward protocol to the destination, and the jamming relay node broadcasts an artificial jamming signal. The power allocated to the subcarriers at the forwarding relaying node and the jamming relay node is optimized so the secrecy rate of the CR system is maximized. In the first phase, interference with the PU's communications is caused by transmission of the source. In the second phase, interference with the PU is caused by both the forwarding relaying nodeâĂŹs transmission and the jamming relay node's transmission. Power is allocated in both the first phase and the second phase such that interference with the PU is below the interference threshold.

We assume an underlay CR transmission where the whole PU spectrum is accessible to the CR system, given that interference with the PU system is less than the interference threshold. The interference caused to the PU as well as the interference caused to the CR receiver is managed through interference alignment in power allocation at the source and forwarding relaying node. The overall power allocation at the jamming relay node and forwarding relaying node is designed in a way to align the interference caused to the legitimate transmission is taken into consideration at forwarding relaying node. We assume that instantaneous channel information is available, and channel coefficients for all links are known a priori. Practical considerations, like using statistical channel knowledge or erroneous channel knowledge and finding the gain of the eavesdropper, are outside the scope of this work. PU communications is not considered in this work other than that the interference caused by the CR transmission should be less than an interference constraint. The physical medium is accessed via OFDM, and thus, all the links have multiple orthogonal subcarriers.

In the first phase, the CR source transmits to the relay network, and the transmission rate at the forwarding relaying node, denoted by R_r, is given by [2]

$$R_r = \log_2(1+\gamma) \tag{1}$$

where $\gamma = \frac{\sum_{i=1}^{N} P_i^s |h_i^{sr}|^2}{N_0}$ is the power allocated at the source to the i-th subcarrier, is the channel gain between source and forwarding relaying node for the i-th subcarrier, N is the total number of subcarriers, and is additive white Gaussian noise (AWGN). In the second phase, the forwarding relaying node forwards the received message to the destination. The transmission rate at the CR receiver, R_e, is given by [2][33]

$$R_d = \frac{1}{2}\log\left[1+\frac{P_s}{N_0}\left(\frac{\left(\frac{\sum_{i=1}^{N}|h_i^{sr}h_i^{rd}|\sqrt{P_i^r}}{\sqrt{P_i^s}|h_i^{sr}|^2+N_0}\right)^2}{1+\sum_{i=1}^{N}\left(\frac{|h_i^{rd}|\sqrt{P_i^r}|h_i^{je}|\sqrt{P_i^j}}{\sqrt{P_i^s}|h_i^{sr}|^2+N_0}\right)^2}\right)\right] \tag{2}$$

where P_s is the combined power as allocated to all subcarriers at the source, h_i^{rd} is the channel gain for the i-th subcarrier between the forwarding relaying node and destination, P_i^r is the power allocated to the i-th subcarrier at the forwarding relaying node, h_i^{je} is the channel gain between the jamming relay node and the eavesdropper for the i-th subcarrier, P_i^j is the power allocated to the i-th subcarrier at the jamming relay node, and the factor $\frac{1}{2}$ is due to two time slots taken for a complete transmission from source to destination. The eavesdropper also receives the signal from the forwarding relaying node along with the jamming signal. The eavesdropper may be able to extract some useful information from the received signal. The transmission rate or throughput at the eavesdropper is represented by and is given as [2], [33]

$$R_e = \frac{1}{2}\log\left[1+\frac{P_s}{N_0}\left(\frac{\left(\frac{\sum_{i=1}^{N}|h_i^{sr}h_i^{re}|\sqrt{P_i^r}}{\sqrt{P_i^s}|h_i^{sr}|^2+N_0}\right)^2}{1+\sum_{i=1}^{N}\left(\frac{|h_i^{re}|\sqrt{P_i^r}|h_i^{je}|\sqrt{P_i^j}}{\sqrt{P_i^s}|h_i^{sr}|^2+N_0}\right)^2}\right)\right] \tag{3}$$

where h_i^{re} is the channel gain of the link between the forwarding relaying node and the eavesdropper for the i-th subcarrier. The secrecy rate is denoted by R_{sec} and by definition is given as [2]

$$R_{\text{sec}} = [R_d - R_e]^+ \tag{4}$$

where $[.]^+$ identifies that the secrecy rate cannot be negative i.e. $R_{\text{sec}} = \max[R_d - R_e, 0]$.

Our main objective is to maximize the secrecy rate of the CR system, as given in (4). In the next section, the constraints on the maximization problem are explained.

B. SYSTEM CONSTRAINTS DEFINITIONS

Each subcarrier from the first hop is mapped to one subcarrier from the other hop. As explained earlier, channel condition for a subcarrier over one hop may change over the next hop. So, instead of forwarding the data received at the forwarding relaying node using the same subcarrier, the channel conditions of the link from forwarding relaying node to destination and forwarding relaying node to eavesdroppers can be taken into consideration in subcarrier mapping at the forwarding relaying node. We exploit this phenomenon to maximize the secrecy rate of the CR system. Let us define a binary mapping variable as

$$\ell_{(k,m)} = \begin{cases} 1, & \text{if } k\text{-th subcarrier of the first hop is assigned} \\ & \text{to } m\text{-th subcarrier of the second hop} \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Another form of subcarrier mapping function can be given as

$$\sum_{k=1}^{N}\ell_{(k,m)} = 1, \quad \forall \text{m}, \quad \sum_{m=1}^{N}\ell_{(k,m)} = 1, \ \forall k. \tag{6}$$

To ensure long-term power availability, the transmission power at the source, the forwarding relaying node, and the jamming relay node should satisfy a maximum power constraint. The maximum power constraint also takes into account the current amount of power available when determining the optimal transmit power. The power constraint at the source is given as

$$0 \le P_i^s \le P_s^{max} \tag{7}$$

where P_s^{max} is the maximum power available at the CR source. The power constraint at the forwarding relaying node and jamming relay node, respectively, are given as

$$0 \le P_i^r \le P_r^{max} \tag{8}$$

and

$$0 \le P_i^j \le P_j^{max} \tag{9}$$

where P_r^{max} is the maximum power available at the forwarding relaying node, and P_j^{max} is the maximum power available at the jamming relay node.

Under our system model, interference with the PU transmission is caused in both the first phase and the second phase of communications. The interference caused in the first phase is because of the source transmission, and so, the transmission should satisfy the maximum interference limit, which is given as

$$\sum_{i=1}^{N}|g_i^s|^2 P_i^s \le I_{max} \tag{10}$$

where I_{max} is the maximum allowable interference threshold, and g_i^s is the channel gain between the source and PU transmitter for the i-th subcarrier. In the second phase, the interference is caused by both forwarding relaying node and jamming

relay node transmissions. The combined interference caused in the second phase should satisfy the maximum allowable interference threshold as

$$\sum_{i=1}^{N} \left|g_i^r\right|^2 P_i^r + \sum_{i=1}^{N} \left|g_i^j\right|^2 P_i^j \leq I_{max} \tag{11}$$

where g_i^r is the channel gain for the i-th subcarrier between the forwarding relaying node and the PU transmitter, and g_i^j is the channel gain for the link between the jamming relay node and the PU transmitter for the i-th subcarrier.

C. PROBLEM FORMULATION

Our aim is to optimize the source power, forwarding relaying node power, and jamming relay node power, and to map subcarriers of the two hops so as to maximize the secrecy rate of the CR system. Power allocation in our system model is not a trivial problem. In traditional OFDM systems and in overlay CRNs, where the CR users access the spectrum if it is not used by the PU, the increase in power allocation increases the system throughput. But in our system model, increasing the power at the source may cause an increase in interference with the PU transmission. An increase in power at the forwarding relaying node may increase interference with the PU as well, and may result in higher leakage to the eavesdropper; and increasing the transmission power at the jamming relay node may result in higher interference with the CR receiver, as well as increase interference with the PU transmission.

The optimization variables for the subcarriers on the first hop (i.e. for source-forwarding relaying node link and for the second hop (i.e. for forwarding relaying node-destination link) can be given mathematically as,$P^s = \left\{P_i^s \geq 0\right\}$, $P^r = \left\{P_i^r \geq 0\right\}$ and $P^j = \left\{P_i^j \geq 0\right\}$ where $\ell = \{\ell_{(k,m)} \in \{0, 1\}\}$ is a vector representing the power allocated to the subcarriers at the CR sender, is a vector representing power allocated to the subcarriers at the forwarding relaying node while is a vector representing power allocated to the subcarriers at the jamming relay node. With these optimization variables, the optimization problem (OP) is given as

$$OP: \quad \max_{\max P^s, P^r, P^j, \ell} \sum_{k=1}^{N} \sum_{m=1}^{N} \ell_{(k,m)} R_{\text{sec}}(k, m)$$
$$s.t.\ (6) - (11). \tag{12}$$

III. POWER ALLOCATION AND SUBCARRIER MAPPING SCHEME

The OP as presented in (12) is divided into four sub-problems. The first sub-problem is to allocate optimal power to the subcarriers at the forwarding relaying node, the second sub-problem is to allocate optimal power at the jamming relay node, the third sub-problem becomes optimal power allocation at the source, and the fourth sub-problem is optimal subcarrier mapping.

$$P^* = \max_{\max P^s, P^r, P^j} \sum_{k=1}^{N} \sum_{m=1}^{N} R_{\text{sec}}(k, m)$$
$$s.t.\ (7) - (11) \tag{13}$$

where $P^* = \{P_s^*, P_r^*, P_j^*\}$. P_s^* is is the optimal source power vector, P_r^* is the optimal power at the forwarding relaying node vector, and P_j^* is is the optimal power vector at the jamming relay node as allocated to the subcarriers.

We consider optimal power allocation at the forwarding relaying node the first sub-problem. In [37] a transmission rate optimization problem was formulated as a mixed-integer nonlinear programming (MINLP) problem. The problem was solved by optimizing the signal to nose ratio (SNR) part of the transmission rate optimization problem. In [37] as the transmission rate function is a monotonically increasing function of the logarithm so the maximized SNR function is put into it to have a solution to the optimization problem. Likewise, the logarithm in (13) is a monotonically increasing function and thus the power allocation parts of (13) have to be optimized to have a solution to the optimization problem. Since the logarithm in (32) is a monotonically increasing function of power, the power allocation parts can be separated, and the OP in terms of power allocation can be given as

$$P_r^* = \arg \max_{P_r} \left\{ \frac{P_s}{N_0} \left(\frac{\left(\sum_{i=1}^{N} \frac{|h_i^{sr} h_i^{rd}| \sqrt{P_i^r}}{\sqrt{P_i^s}|h_i^{sr}|^2 + N_0} \right)^2}{1 + \sum_{i=1}^{N} \left(\frac{|h_i^{rd}| \sqrt{P_i^r} |h_i^{je}| \sqrt{P_i^j}}{\sqrt{P_i^s}|h_i^{sr}|^2 + N_0} \right)^2} \right) \right\}$$
$$\text{s.t. (8) and (11).} \tag{14}$$

For the sake of simplicity, let $\alpha_i = \left|h_i^{sr}\right|^2$, $\beta_i = \left|h_i^{rd}\right|^2$, $\lambda_i = \left|h_i^{jd}\right|^2$, $w_i = \left|g_i^r\right|^2$, $v_i = \left|g_i^j\right|^2$, $\sigma_i = \frac{P_i^j}{P_i^r}$, $u_i = \frac{v_i P_i^j}{\sigma_i}$ and $\gamma_i = \frac{\beta_i}{\alpha_i P_i^s + N_0}$. Equation (14) can be expressed in terms of α_i, β_i, λ_i, w_i, v_i and γ_i as

$$P_r^* = \arg \max_{P^r = \{P_1^r, P_2^r, \ldots, P_N^r\}} \frac{\left(\sum_{i=1}^{N} \left(\sqrt{\alpha_i \gamma_i} \sqrt{P_i^r} \sqrt{P_i^j} \right) \right)^2}{1 + \sum_{i=1}^{N} \gamma_i \lambda_i P_i^r P_i^j} \tag{15}$$

$$\text{subject to } 0 \leq P_i^r \leq P_{\max}^r \tag{16}$$

and

$$\sum_{i=1}^{N} (w_i P_i^r + v_i P_i^j) \leq I_{\max}. \tag{17}$$

The objective function in (15) is a non-convex function of P_i^r. It is difficult to obtain a global optimal solution. The local optimal solution can be obtained by using the

integer point method (IPM). The transmission power at the forwarding relaying node is not only restricted by maximum transmission power but also by the maximum interference constraint. In order to simplify the optimization problem, the maximum power constraint at the forwarding relaying node as is given in (16) can be relaxed at first. After a closed form solution for the simplified problem in (15) is obtaining using the Cauchy-Shwartz inequality, then the maximum transmission power constraint at the forwarding relaying node will be guaranteed.

To solve the optimal power allocation at the forwarding relaying node, the constraint given in (17) is used as the only constraint on the optimization problem in (15). The optimal solution of (15) is not possible if the constraint in (17) is not followed with strict equality. If the constraint in (15) is not followed by strict equality then for every solution there can exist another solution which is a linear combination of the previous solution. The new solution can be obtained by multiplying the previous solution with a constant C and which will result in higher value of the objective function in (15). Thus, (17) becomes

$$\sum_{i=1}^{N} \left(w_i P_i^r + v_i P_i^j\right) = I_{\max}. \tag{18}$$

Using (17), the objective function in (15) can be written as in (19);

$$\begin{aligned}\frac{\left(\sum_{i=1}^{N}\left(\sqrt{\alpha_i\gamma_i}\sqrt{P_i^r}\sqrt{P_i^j}\right)\right)^2}{1+\sum_{i=1}^{N}\gamma_i\lambda_i P_i^r P_i^j} &= \frac{\left(\sum_{i=1}^{N}\left(\sqrt{\alpha_i\gamma_i}\sqrt{P_i^r}\sqrt{P_i^j}\right)\right)^2}{\frac{\sum_{i=1}^{N}\left(w_i P_i^r + v_i P_i^j\right)}{I_{\max}} + \sum_{i=1}^{N}\gamma_i\lambda_i P_i^r P_i^j} \\ &= \frac{\left(\sum_{i=1}^{N}\left(\sqrt{\alpha_i\gamma_i}\sqrt{P_i^r}\sqrt{P_i^j}\right)\right)^2}{\sum_{i=1}^{N}\left\{\left(\frac{\frac{w_i}{P_i^j}+\frac{v_i}{P_i^r}}{I_{\max}}+\gamma_i\lambda_i\right)P_i^r P_i^j\right\}}.\end{aligned} \tag{19}$$

To express (19) simply, we define two new variables as

$$z_i = \sqrt{\left(\gamma_i\lambda_i + \frac{W_i+V_i}{I_{\max}}\right)}\sqrt{P_i^r P_i^j} \tag{20}$$

and

$$d_i = \sqrt{\frac{\alpha_i\gamma_i}{\lambda_i\gamma_i + \frac{W_i+V_i}{I_{\max}}}} \tag{21}$$

where $W_i = \frac{w_i}{P_i^j}$ and $V_i = \frac{v_i}{P_i^r}$. Two vectors are formed as $z = [z_i]$ and $d = [d_i]$. The two vectors can be used to represent the objective function in (18) in vector form [31]. The objective function in (18) can be represented in vector form as

$$P_r^* = \arg \max_{z=f(p^r)} \frac{\left(d^T z\right)^2}{z^T z}. \tag{22}$$

The optimal solution of (22) can be found by the Cauchy-Shwartz inequality. Furthermore according to [37], the optimal solution can then be given if z and d are linearly independent as

$$z_i^* = k d_i. \tag{23}$$

Putting value of d_i from (21), eq. (23) becomes

$$\left(z_i^*\right)^2 = k^2\left(\frac{\alpha_i\gamma_i}{\lambda_i\gamma_i + \frac{W_i+V_i}{I_{\max}}}\right). \tag{24}$$

Eq. (20) can be written for z_i^* as

$$\begin{aligned}\left(z_i^*\right)^2 &= \left(\gamma_i\lambda_i + \frac{W_i+V_i}{I_{\max}}\right)P_i^r P_i^j \\ \left(z_i^*\right)^2 I_{\max} &= \left(I_{\max}\gamma_i\lambda + W_i + V_i\right)P_i^r P_i^j \\ P_i^r P_i^j &= \frac{\left(z_i^*\right)^2 I_{\max}}{I_{\max}\gamma_i\lambda + W_i + V_i} \\ \left(W_i+V_i\right)P_i^r P_i^j &= \frac{\left(z_i^*\right)^2 I_{\max}}{I_{\max}\gamma_i\lambda + W_i + V_i}\left(W_i+V_i\right) \\ \left(z_i^*\right)^2 &= \frac{\left\{\left(W_i+V_i\right)P_i^r P_i^j\right\}\left\{I_{\max}\gamma_i\lambda + W_i + V_i\right\}}{I_{\max}\left(W_i+V_i\right)}.\end{aligned} \tag{25}$$

Eq. (24) can be rewritten when the value of $\left(z_i^*\right)^2$ from (25) is put into it as

$$\begin{aligned}\left(w_i P_i^r + v_i P_i^j\right) &= k^2\left(\frac{\alpha_i\gamma_i}{I_{\max}\lambda_i\gamma_i + W_i + V_i}\right) \\ &\quad \times \frac{I_{\max}^2}{I_{\max}\gamma_i\lambda + W_i + V_i}\left(W_i+V_i\right) \\ 1 &= \frac{k^2\alpha_i\gamma_i I_{\max}(W_i+V_i)}{\left(I_{\max}\lambda_i\gamma_i + W_i + V_i\right)^2}.\end{aligned} \tag{26}$$

From (26), for the N subcarriers, k can be given as

$$k = \sqrt{\frac{1}{I_{\max}\sum_{i=1}^{N}\frac{(W_i+V_i)\alpha_i\gamma_i}{\{(W_i+V_i)+\gamma_i\lambda_i I_{\max}\}^2}}}. \tag{27}$$

If $P_{r_i}^*$ is the optimal power allocated to each subcarrier at the forwarding relaying node, then $P_{r_i}^*$ can be represented in terms according to (20) as

$$\begin{aligned}P_{r_i}^* &= \frac{\left(z_i^*\right)^2}{\lambda_i\gamma_i + \frac{(W_i+V_i)}{I_{\max}}P_i^j} \\ &= \frac{k^2\frac{\alpha_i\gamma_i}{I_{\max}\lambda_i\gamma_i+(W_i+V_i)}I_{\max}^2}{I_{\max}\lambda_i\gamma_i + (W_i+V_i)P_i^j}.\end{aligned} \tag{28}$$

Putting value of k, $P^*_{r_i}$ becomes

$$P^*_{r_i} = \left(\frac{1}{I_{\max}\sum_{i=1}^{N}\frac{(W_i+V_i)\alpha_i\gamma_i}{\{(W_i+V_i)+\gamma_i\lambda_i I_{\max}\}^2}}\right) \times \left(\frac{\alpha_i\gamma_i I^2_{\max}}{\{I_{\max}\lambda_i\gamma_i+(W_i+V_i)\}^2 P^j_i}\right) = I_{\max}\frac{\frac{\alpha_i\gamma_i}{((w_i+u_i)+\gamma_i I_{\max})^2}}{\sum_{i=1}^{N}\frac{(w_i+v_i)\alpha_i\gamma_i}{\{(w_i+u_i)+\gamma_i\lambda_i I_{\max}\}^2}}. \quad (29)$$

The equation in (29) satisfies the maximum interference constraint only, i.e. the constraint given in (17). To satisfy the constraints in (16) (i.e. the maximum transmission power constraint), we propose optimal power allocation at the forwarding relaying node to each subcarrier, represented by $P^{proposed}_{r_i}$, which is given as

$$P^{proposed}_{r_i} = \min\left(P^r_{max}, P^*_{r_i}\right). \quad (30)$$

In sub-problem 2, the power at the jamming relay node is allocated. The power to all subcarriers at the jamming relay node is allocated equally. Joint optimization of both forwarding relaying node and jamming relay node becomes intractable. The jamming signal affects the signal received by the eavesdropper more than it affects the signal received at the destination. The power allocated at the jamming relay node to each subcarrier is represented by $P^{proposed}_{j_i}$ and is given as

$$P^{proposed}_{j_i} = \eta\frac{P^{total}_j}{N} \quad (31)$$

where P^{total}_j is the power available at the jamming relay node, η is a factor that maintains the allocated power at the jamming relay node such that it satisfies (11), and η is selected iteratively.

In sub-problem 3, power is allocated to each subcarrier at the source, represented by $P^{proposed}_{s_i}$, as

$$P^{proposed}_{s_i} = \chi\frac{I_{\max}}{g^{sp}_i} \quad (32)$$

where χ ensures that the allocated power satisfies the maximum transmission power constraint in (7). The maximum interference constraint as given in (10) is implicitly satisfied by (32). By (32), more power is allocated to links with a good channel condition, and thus, CR system throughput is increased.

In the sub-problem 4, the subcarriers are matched. The channel gain from forwarding relaying node to CR receiver and the channel gain from forwarding relaying node to eavesdropper are good parameters, on the basis of which the secrecy rate can be optimized. In the Algorithm 1, S is a vector that represents all the subcarriers from the CR source to the forwarding relaying node, C is a vector that represents all the subcarriers from the forwarding relaying node to the destination, h^{sr} is a vector that represents the channel gain for all subcarriers from the source to the forwarding relaying node, h^{rd} is a vector that represents the channel gain for all subcarriers from the forwarding relaying node to the destination, and h^{re} is a vector that represents the channel gain for all subcarriers from forwarding relaying node to eavesdropper. The ratio Λ_i is found out for all the subcarriers from the forwarding relaying node to the destination to calculate the ratio between the gain from the forwarding relaying node to destination and the gain from the forwarding relaying node to eavesdroppers for the subcarriers. Subcarriers having larger value of Λ_i have better gain from forwarding relaying node to destination than from forwarding relaying node to the eavesdropper and hence are better channels. This fact is exploited to map the better subcarriers from source to forwarding relaying node with subcarriers from forwarding relaying node to destination.

The complexity of the proposed algorithm in Algorithm 1 is $O(N)$ where N is the number of subcarriers. Because of the ratio vector Λ as introduced in Algorithm 1, one subcarrier from the CR sender to the forwarding relaying node is matched with a subcarrier from the forwarding relaying node to CR destination in only one iteration. The subcarrier with the maximum channel gain from the CR sender to the forwarding relaying node is matched with the subcarrier from forwarding relaying node to the CR destination which has the best ratio of channel gain from forwarding relaying node to the CR destination to the channel gain from forwarding relaying node to the eavesdropper. Thus, the mapping will be completed in N steps.

The solution to the optimization problem as presented in (12) is provided by the equations in (29), (30), (31), and Algorithm 1. Eq. (29) presents solution to the first sub-problem which is allocation of power at the forwarding relaying node, (30) provides solution to the second sub-problem which is to allocate power at the jamming relay node, (31) gives solution to the third sub-problem which is to allocate power at the source while Algorithm 1 presents solution to the fourth sub-problem which is subcarrier mapping at the forwarding relaying node. Finally, Fig. 2 shows the flowchart of the proposed scheme. The labels on the right of the blocks in the flowchart represent the node at which the operation is carried out. At the forwarding relaying node both Algorithm 1 and the power allocation to subcarriers according to (31) are carried out.

IV. RESULTS AND DISCUSSION

We carried out a number of simulations to verify the performance of our proposed scheme. The simulation platform used was Matlab R2017a. We assumed that the channel coefficients undergo Rayleigh fading. We also assumed that all the subcarriers face independent Rayleigh fading, both in the CR system and from the CR system to the PU system, and that the channel gains are also independent from each other. A fixed broadband wireless channel with 1 MHz bandwidth is assumed for the simulation. The noise spectrum density is set to $4.14\text{x}10^{-21}$ W/Hz [20]. The path loss exponent in the Rayleigh fading model is considered to be 4 which represents

Algorithm 1 Algorithm 1

$S = \{S_1, S_2, ..., S_N\}$
$C = \{C_1, C_2, ..., C_N\}$
Input: $|h^{sr}| = \left\{\left|h_1^{sr}\right|, \left|h_2^{sr}\right|, ..., \left|h_N^{re}\right|\right\}$
$|h^{re}| = \left\{\left|h_1^{re}\right|, \left|h_2^{re}\right|, ..., \left|h_N^{re}\right|\right\}$
$\left|h^{rd}\right| = \left\{\left|h_1^{rd}\right|, \left|h_2^{rd}\right|, ..., \left|h_N^{rd}\right|\right\}$

1. Find $\Lambda_i = \frac{|h_i^{rd}|}{|h_i^{re}|}$ where $i = \{1, 2, ..., N\}$. Form a vector as $\Lambda = \{\Lambda_1, \Lambda_2, ..., \Lambda_N\}$.

2. From $|h^{sr}|$ find $\left|h_i^{sr}\right| = \max\{|h^{sr}|\}$. The subcarrier having the channel gain $\left|h_i^{sr}\right|$ is S_i. From Λ find $\Lambda_j = \max\{\Lambda\}$. The subcarrier corresponding to Λ_j is C_j. Remove S_i from S, C_j from C, $\left|h_i^{sr}\right|$ from $|h^{sr}|$ and Λ_j from Λ.

3. Map S_i and C_j as
$S_i \leftrightarrow C_j$

4. if $S \neq \emptyset$ and $C \neq \emptyset$
Go to Step 2

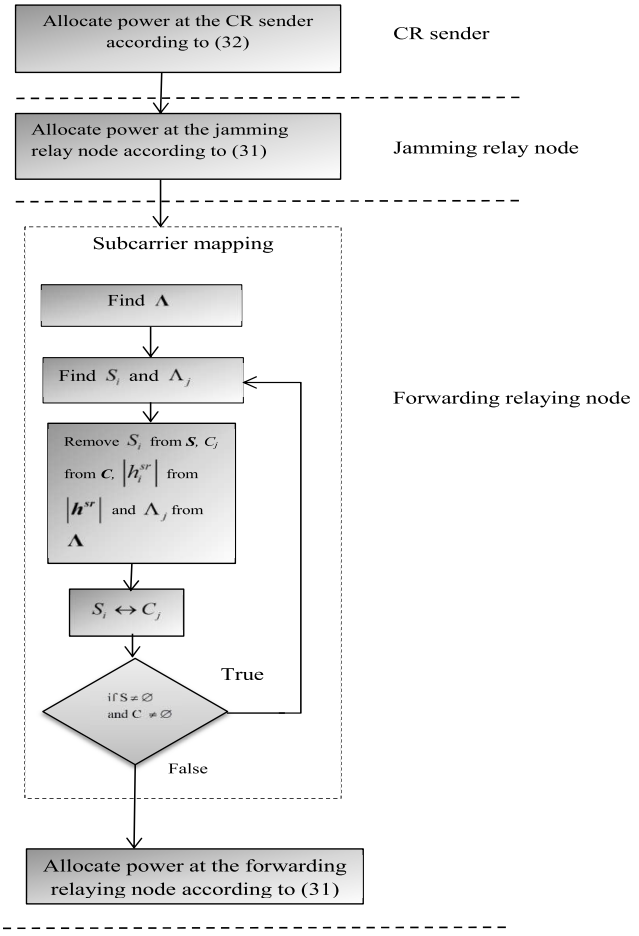

FIGURE 2. Flowchart of the proposed scheme.

worst case scenarios for cellular and long-distance communications and as the value of the path loss exponent reduces, the corresponding performances can be improved [38], [39].

In the simulation, the product of spectrum bandwidth and time period is assumed to be one unit. The maximum transmission power constraint is assumed to be the same at the CR source, the forwarding relaying node, and the jamming relay node, for the sake of simplicity. Some of the simulation parameters are summarized in Table 1.

TABLE 1. Parameters used for simulation.

Parameter	Value
Wireless channel bandwidth	1 MHz
Noise spectrum density	$4.14x10^{-21}$ W/Hz
Path loss exponent	4
Distance between the source and relay network (for fig. 3,4 and 6)	200 m
Distance between the relay network and destination (for fig. 3,4, 6 and 7)	300 m
Distance between the relay network and eavesdropper (for fig. 3,4, 6 and 7)	250 m
Maximum interference threshold (for fig. 3 and 7)	5 dBm
Maximum interference threshold (for fig. 4, 6 and 6)	3 dBM
Maximum transmission power (for fig. 3,5,6 and 7)	10 W

We consider three types of schemes, against which we compare our proposed scheme. The first scheme is a mapping with equal power allocation scheme, which is a variant of our proposed system model, but the power is equally allocated among all subcarriers at the source, forwarding relaying node, and jamming relay node, and sub-carrier mapping is done at the forwarding relaying node, based on Algorithm 1. The interference threshold and maximum transmission power are always the same in this scheme, as in our proposed scheme. The other scheme is a baseline half-duplex scheme, as presented by Zheng *et al.* [4]. We call this scheme the baseline scheme where we have one relay that forwards the received information without any optimization, and the power is allocated at the relay under the maximum transmission power constraint and maximum interference constraint. The throughput rate at the destination for the baseline scheme is represented by R_d^b, and the throughput rate at the eavesdropper is represented by R_e^b, which are given as

$$R_d^b = \frac{1}{2} log \left\{1 + \sum_{i=1}^{N} P_i^s \left|h_i^{sr}\right|^2 P_i^r \left|h_i^{rd}\right|^2\right\} \tag{33}$$

and

$$R_e^b = \frac{1}{2} log \left\{1 + \sum_{i=1}^{N} P_i^s \left|h_i^{sr}\right|^2 P_i^r \left|h_i^{re}\right|^2\right\} \tag{34}$$

respectively. The secrecy rate for the baseline scheme is represented by R_{sec}^b, and is given as

$$R_{\text{sec}}^b = R_d^b - R_e^b. \tag{35}$$

The third scheme is an exhaustive search scheme. In this scheme, mapping of subcarriers is carried out based on Algorithm 1, and the power in the feasible search space for power allocation is exhaustively searched for all subcarriers at the forwarding relaying node to allocate optimal transmit power to the subcarriers. This can be considered the upper

bound for our proposed scheme. The simulation parameters are given in detail in Table I.

For Fig. 3, Fig. 4, and Fig. 6, the distances between different nodes for the system model as presented in Figure 1 are as follows. The distance between the source and the relay network is 200 m; the distance between the relay network and the destination is 300 m, and the distance between the relay network and the eavesdropper is 250 m. The maximum interference constraint makes the CR system and PU system coexist, even at a closer distance.

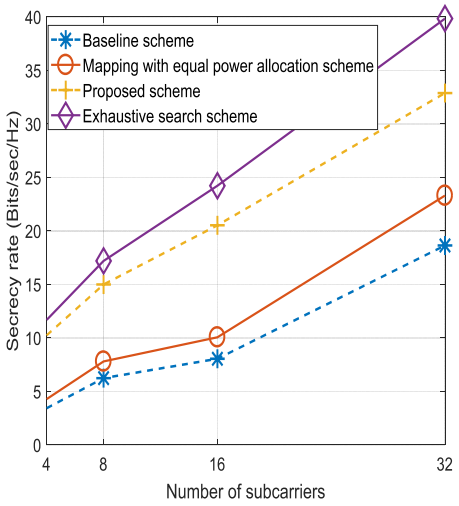

FIGURE 3. Effect of number of subcarriers on secrecy rate.

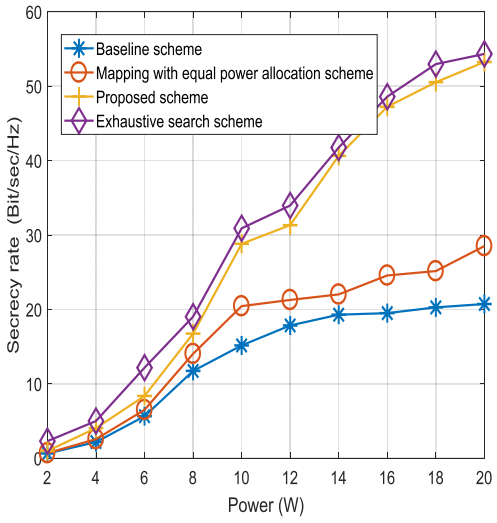

FIGURE 4. Effect of maximum transmission power on secrecy rate.

Fig. 3 shows the effect of the number of subcarriers on the secrecy rate. The maximum transmission power is 10 W, and the maximum interference threshold is 5 dBm. The secrecy rate of our proposed scheme is higher than both of the other schemes. With an increase in the number of subcarriers, there is a steep increase in the performance of our proposed scheme. The baseline scheme does not greatly benefit from increasing the number of subcarriers because of the increased leakage to the eavesdropper. The exhaustive search scheme outperforms our proposed scheme but at the cost of computational complexity and computation time.

Fig. 4 presents the effect of maximum transmission power at the source, forwarding relaying node, and jamming relay node for 32 subcarriers, and the maximum interference threshold is 3 dBm. It is clear from Fig. 4 that with an increase in the transmission power, the secrecy rate also increases. From Fig. 4, it can be seen that after a certain amount of maximum transmission power, the secrecy rate becomes stable (i.e. the secrecy rate does not increase with further increases in maximum transmission power). This is because of the interference constraint. As the maximum transmission power increases, so does the interference with the PU, and when the interference limit is reached, transmit power is not increased despite the fact that the maximum transmission power limit may not have been reached. Our proposed scheme outperforms the other schemes except for the exhaustive search scheme, but the proposed scheme converges to the upper bound and follows the exhaustive search scheme closely for the whole range of transmission power.

We have tested the proposed scheme for three distances between the relay network and the eavesdropper, as shown in Fig. 5. The distance between the source and the relay network is 200 m, the distance between the relay network and the destination is 300 m [38], and the maximum interference threshold is 3 dBm [1]. Only the distance between the relay network and the eavesdropper was changed. The three cases are as follows.

Case 1: The distance between the relay network and the eavesdropper is 50 m.

Case 2: The distance between the relay network and the eavesdropper is 150 m.

Case 3: The distance between the relay network and the eavesdropper is 250 m.

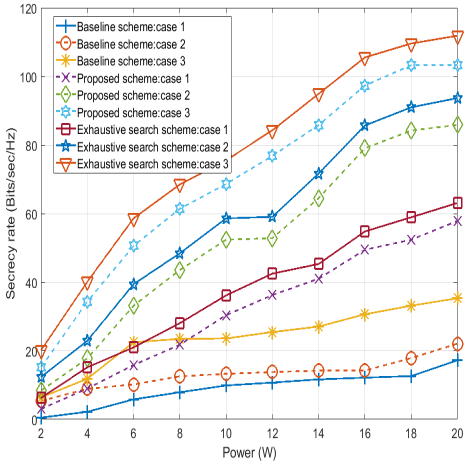

FIGURE 5. Effect of the distance between relay network and eavesdropper on the secrecy rate.

Our proposed scheme performs best when the eavesdropper is closer to the relay network. That is because the jamming relay node signal affects the signal received at the eavesdropper more than the interference caused at the destination. Due to the subcarrier mapping and optimal power allocation at the forwarding relaying node, the eavesdropper receives little information from the forwarding relaying node, even when it is closer. As the eavesdropper moves closer to the destination, the interference caused by the jamming relay node to both the eavesdropper and the destination reaches almost the same level. Thus, the secrecy rate drops when the eavesdropper is nearer the destination. The case for the baseline scheme is different than our proposed scheme. When the eavesdropper is near the forwarding relaying node or near the destination, the secrecy rate is almost the same. In case 1, when the eavesdropper is near the forwarding relaying node, the eavesdropper gets the same information as the CR receiver. In case 2, when the eavesdropper is near the destination, both the eavesdropper and the destination lie on the same line and distance, and hence, both receive the same information. Thus, the secrecy rate drops in this case, too.

In Fig. 6, the complex channel coefficient between the forwarding relaying node and the CR receiver for each subcarrier is calculated as

$$h_i^{rd} = \left|h_i^{rd}\right| .e^{j\theta} \tag{36}$$

where $\left|h_i^{rd}\right|$ is the channel gain between the forwarding relaying node and the destination for the i-th subcarrier, and θ is uniformly distributed in. The average result was obtained using Monte Carlo simulation, which consisted of 1000 trials. The simulation was run using four subcarriers, and the maximum interference threshold was 3 dBm. For simplicity, the complex channels between the other nodes are assumed to be $0.8e^{j\frac{\pi}{4}}$ [4]. In the previous simulation results the channel gains as well as the phase of the channel were kept constant and the results were obtained by changing other parameters. The proposed scheme closely follows the exhaustive search scheme as the number of iterations gets larger, and thus, the average performance of the proposed scheme is near the optimal exhaustive search scheme, but uses less computation power and takes less computation time.

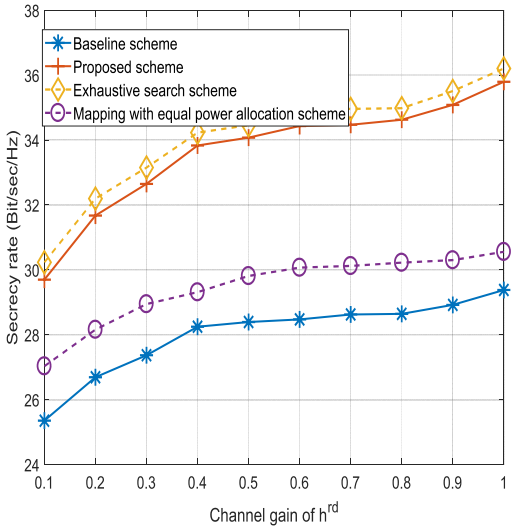

FIGURE 6. Effect of channel gain between relay and CR receiver on the secrecy rate.

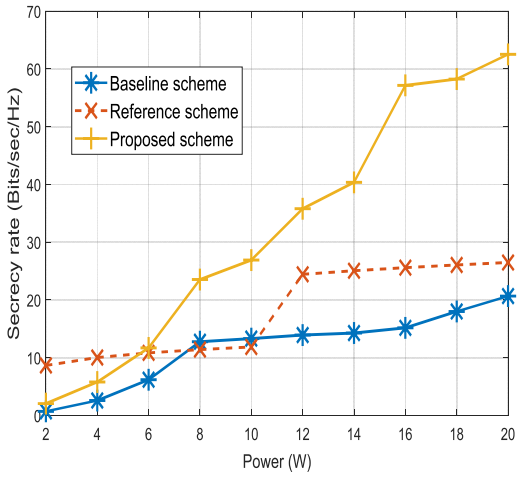

FIGURE 7. Performance comparison among the reference schemes.

For the sake of comparing our scheme with literature, we have taken the scheme presented for secrecy capacity analysis in [40]. The scheme in [40] is similar to our scheme in terms of topology. Therefore, we consider the scheme in [40] as a reference scheme as following: The secrecy rate of the reference scheme for a transmitter-receiver pair is as [40]

$$R_{\text{sec}}^{r} = \max \left\{ \begin{matrix} log_2\left(1 + \frac{P_T}{\|x_i - x_j\|^{\alpha}(B+I_P)}\right) - \\ log_2\left(1 + \frac{P_T}{\|x_i - e^*\|^{\alpha}(B+I_E)}\right), 0 \end{matrix} \right\} \tag{37}$$

where P_T is the transmitted power, $\|x_i - x_j\|$ is the distance between the CR sender and CR destination, B is the noise power induced by the primary receivers to the CR destinations, I_P is the interference caused to the PU receivers by the CR transmissions, $\|x_i - e^*\|$ is the distance between the CR sender and eavesdropper, is the path loss exponent and I_E is the leakage to the eavesdroppers. $\|x_i - x_j\|$ is 300 m, $\|x_i - e^*\|$ is 250m, α is 2. The values of B and I_E are 3 dBm while I_P is 5 dBm. The number of subcarriers is 32. For the reference scheme, the secrecy rate is calculated by summing the rates of 32 different CR sender-CR destination pairs.

V. CONCLUSION

In order to optimize the secrecy rate, power allocation at the source, at the jamming relay node, and at the forwarding relaying node is considered along with subcarrier mapping which makes the leakage to the eavesdropper minimal at the forwarding relaying node in this paper. Power to the subcarriers at the source and the jamming relay node is allocated by taking into consideration the channel gain and satisfying the maximum interference threshold and the maximum power

transmission constraint. The power allocation problem at the forwarding relaying node is non-convex, thus, it is simplified by relaxing the maximum transmission power constraint, and a local solution is obtained using IPM. The maximum power transmission constraint is satisfied after obtaining a local solution. The power allocated at the forwarding relaying node also aligns the interference caused to the CR receiver by the jamming signal by incorporating the power of jamming signal into the power allocation scheme at the forwarding relaying node. We have shown through simulation results that the proposed scheme can significantly enhance the secrecy rate while satisfying the interference constraints put in to safeguard the PU's communications from harmful interference. We also showed that the proposed scheme closely follows the exhaustive search scheme, which is the upper bound for our proposed scheme, while being computationally less complex.

In our future work, we plan to find a joint solution to the optimization problem, where power allocation at the source, at the jamming relay node, and at the forwarding relaying node, and subcarrier mapping will be jointly solved to find an optimal solution to the optimization problem formulated in this paper. The current system model, optimization problem and hence the solution do not take into consideration the effect of multiple eavesdroppers, relays and PUs. Therefore, we also plan to extend the system model to take into consideration multiple eavesdroppers, relays and PUs.

REFERENCES

[1] G. A. S. Sidhu, F. Gao, W. Wang, and W. Chen, "Resource allocation in relay-aided OFDM cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 3700–3710, Oct. 2013.

[2] 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.

[3] L. Ozarow and A. Wyner, "Wiretap channel II," in *Advances Cryptology*. Berlin, Germany: Springer, 1985, pp. 33–50.

[4] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[5] A. K. Sadek, W. Su, and K. J. R. Liu, "Multinode cooperative communications in wireless networks," *IEEE Trans. Signal Process.*, vol. 55, no. 1, pp. 341–355, Jan. 2007.

[6] K. G. Seddik, A. K. Sadek, W. Su, and K. J. R. Liu, "Outage analysis and optimal power allocation for multinode relay networks," *IEEE Signal Process. Lett.*, vol. 14, no. 6, pp. 377–380, Jun. 2007.

[7] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proc. IEEE-ICC*, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.

[8] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE-ICASP*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[9] S. Sarma and J. Kuri, "SNR based secure communication via untrusted amplify-and-forward relay nodes using artificial noise," *Wireless Netw.*, vol. 24, no. 1, pp. 1–12, 2018.

[10] J. Zhang, G. Pan, and H.-M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, Jul. 2016.

[11] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 335–346, Jan. 2017.

[12] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[13] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[14] K. Cumanan *et al.*, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2017.

[15] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[16] I. Krikidis, J. S. 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.

[17] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[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. 3532–3545, Jul. 2012.

[19] K. Lee, C. B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4672–4678, Nov. 2013.

[20] H. Mu, M. Tao, W. Dang, and Y. Xiao, "Joint subcarrier-relay assignment and power allocation for decode-and-forward multi-relay OFDM systems," in *Proc. IEEE 4th Int. Conf. Commun. Netw. ChinaCOM*, Aug. 2009, pp. 1–6.

[21] C. K. Ho, R. Zhang, and Y. C. Liang, "Two-way relaying over OFDM: Optimized tone permutation and power allocation," in *Proc. IEEE-ICC*, Beijing, China, May 2008, pp. 3908–3912.

[22] K. Jitvanichphaibool, Y. C. Liang, and R. Zhang, "Beamforming and power control for multi-antenna cognitive two-way relaying," in *Proc. IEEE Conf. Wireless Commun. Netw.*, Budaptest, Hungary, Apr. 2009, pp. 1–6.

[23] G. Bansal, M. J. Hossain, and V. K. Bhargava, "Adaptive power loading for OFDM-based cognitive radio systems with statistical interference constraint," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2786–2791, Sep. 2011.

[24] S. Yan and X. Wang, "Power allocation for cognitive radio systems based on nonregenerative OFDM relay transmission," in *Proc. IEEE 5th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Beijing, China, Sep. 2009, pp. 1–4.

[25] J. Jia, J. Zhang, and Q. Zhang, "Cooperative relay for cognitive radio networks," in *Proc. IEEE-INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 2304–2312.

[26] M. Herdin, "A chunk based OFDM amplify-and-forward relaying scheme for 4G mobile radio systems," in *Proc. IEEE-ICC*, Istanbul, Turkey, vol. 10, Jun. 2006, pp. 4507–4512.

[27] I. Hammerstrom and A. Wittneben, "Power allocation schemes for amplify-and-forward MIMO-OFDM relay links," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2798–2802, 2007.

[28] Y. Li, W. Wang, J. Kong, and M. Peng, "Subcarrier pairing for amplify-and-forward and decode-and-forward OFDM relay links," *IEEE Commun. Lett.*, vol. 13, no. 4, pp. 209–211, Apr. 2009.

[29] C. M. Yetis, T. Gou, S. A. Jafar, and A. H. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4771–4782, Sep. 2010.

[30] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[31] M. Choi, J. Park, and S. Choi, "Simplified power allocation scheme for cognitive multi-node relay networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2008–2012, Jun. 2012.

[32] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[33] D. W. K. Ng, M. Shaqfeh, R. Schober, and H. Alnuweiri, "Robust layered transmission in secure MISO multiuser unicast cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8267–8282, Oct. 2015.
[34] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2450–2464, Apr. 2017.
[35] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo. (2018). "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT." [Online]. Available: https://arxiv.org/abs/1802.09609v1
[36] Y. Huang, Z. Li, and R. Zui, "Robust AN-aided beamforming design for secure MISO cognitive radio based on a practical nonlinear EH model," *IEEE Access*, vol. 5, pp. 14011–14019, 2017.
[37] Z. Zhou and Q. Zhu, "Joint optimization scheme for power allocation and subcarrier pairing in OFDM-based multi-relay networks," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1039–1042, Jun. 2014.
[38] J. Dorleus, R. Holweck, Z. Ren, H. Li, H. -L. Cui, and J. Medina, "Modeling and simulation of fading and pathloss in opnet for range communications," in *Proc. IEEE Radio Wireless Symp.*, Long Beach, CA, USA, Jan. 2007, pp. 407–410, doi: 10.1109/RWS.2007.351854.
[39] F. Gabry, A. Zappone, and R. Thobaben, "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 437–440, Aug. 2015.
[40] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

HURMAT ALI SHAH received the B.Sc. and M.Sc. degrees in computer systems engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2010 and 2013, respectively. He is currently pursuing the Ph.D. degree with the Multimedia Communications System Laboratory, University of Ulsan, South Korea. His research interests include secure spectrum sensing in cognitive radio networks, next generation communications, and wireless sensor networks.

INSOO KOO received the B.E. degree from Kon-Kuk University, Seoul, South Korea, in 1996, and the M.S. and Ph.D. degrees from the Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 1998 and 2002, respectively. From 2002 to 2004, he was with the Ultrafast Fiber-Optic Networks Research Center, GIST, as a Research Professor. In 2003, he was a Visiting Scholar with the Royal Institute of Science and Technology, Stockholm, Sweden. In 2005, he joined the University of Ulsan, South Korea, where he is currently a Full Professor. His current research interests include next generation wireless communication systems and wireless sensor networks.