รายงานวิจัยฉบับสมบูรณ์

โครงการการเข้ารหัสเครือข่ายไร้สายสำหรับการระบุตำแหน่งในร่ม แบบร่วมมือในเครือข่ายวิทยุที่มีการเรียนรู้

โดย ผู้ช่วยศาสตราจารย์ ดร.กำพล วรดิษฐ์

สิงหาคม พ.ศ. 2563

สัญญาเลขที่ MRG5680177

รายงานวิจัยฉบับสมบูรณ์

โครงการการเข้ารหัสเครือข่ายไร้สายสำหรับการระบุตำแหน่งในร่ม แบบร่วมมือในเครือข่ายวิทยุที่มีการเรียนรู้

โดย ผู้ช่วยศาสตราจารย์ ดร.กำพล วรดิษฐ์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

สนับสนุนโดยสำนักงานกองทุนสนับสนุนการวิจัยและ
มหาวิทยาลัยศรีนครินทรวิโรฒ

(ความเห็นในรายงานนี้เป็นของผู้วิจัย
สกว.และมศวไม่จำเป็นต้องเห็นด้วยเสมอไป)

บทคัดย่อ

ความต้องการในการใช้เครือข่ายสื่อสารไร้สายเพิ่มขึ้นอย่างรวดเร็ว ทั้งในแง่ความเร็ว พื้นที่ครอบคลุมของสัญญาณ ความเป็นส่วนตัว และความปลอดภัย อย่างไรก็ดี การทำให้ได้ตามเป้าหมายดังกล่าวเป็นเรื่องยาก เนื่องจากลักษณะธรรมชาติของเครือข่ายสื่อสารไร้สายสองประการ ได้แก่ แบนด์วิดท์ที่จำกัด และการส่งสัญญาณที่เป็นแบบแพร่กระจาย ในประเด็นแบนด์วิดท์ที่จำกัด นักวิจัยต้องหาเทคนิคที่สามารถปรับปรุงประสิทธิภาพการใช้งานแบนด์วิดท์ เพื่อให้สามารถส่งข้อมูลในปริมาณที่มากขึ้นได้ โดยใช้ปริมาณแบนด์วิดท์เท่าเดิมที่มีอยู่ เทคนิคที่น่าสนใจได้แก่ วิทยุที่มีการเรียนรู้ และการสื่อสารโดยใช้การระบุตำแหน่งเข้าช่วย และวิทยุที่มีการเรียนรู้สามารถทำให้มีประสิทธิภาพสูงขึ้นได้อีกด้วยการใช้การสื่อสารแบบร่วมมือเข้าเสริม ในประเด็นการส่งสัญญาณที่เป็นแบบแพร่กระจาย ความเป็นส่วนตัวและความปลอดภัยของผู้ใช้ในเครือข่ายสื่อสารไร้สายถูกลดทอนลง นักวิจัยจำเป็นต้องหาเทคนิคปรับปรุงอัตราเร็วในการส่งข้อมูลที่เป็นความลับ เพื่อว่าผู้ใช้งานในเครือข่ายสื่อสารไร้สาย สามารถส่งข้อมูลได้อย่างเป็นความลับ ด้วยความเร็วที่สูงในระดับที่สมเหตุสมผล ในงานวิจัยนี้ได้นำเสนอเทคนิคการเข้ารหัส ซึ่งสามารถปรับปรุงประสิทธิภาพการใช้งานแบนด์วิดท์ จากนั้นจึงนำเสนอเทคนิคการใช้การระบุตำแหน่งเข้าช่วยในการสื่อสารแบบร่วมมือเพื่อให้มีการใช้งานแบนด์วิดท์ได้มีประสิทธิภาพสูงขึ้น นอกจากนี้ยังนำเสนอกรอบงานในการหาค่าเหมาะสมที่สุด เพื่อให้ได้อัตราเร็วในการส่งข้อมูลที่เป็นความลับสูงที่สุดสำหรับเครือข่ายสื่อสารไร้สาย ภายใต้ข้อจำกัดที่อุปกรณ์รับสัญญาณไม่มีแหล่งพลังงานในตัวเอง

Abstract

The demands in wireless communication network dramatically increase in terms of speed, coverage, privacy, and security. However, meeting those goals is difficult due to two natures of wireless communication networks, namely, limited bandwidth and broadcasting transmission. As per the limited bandwidth, researchers need to find the techniques that can improve the efficiency of bandwidth utilization so that more amount of data can be transmitted using the available amount of bandwidth. The interesting techniques include cognitive radios and positioning-aided communications, and the cognitive radios can be further enhanced by cooperative communications. As per the broadcasting transmission, the privacy and security of the users in the wireless communication networks are compromised. The researchers need to find the techniques that can improve the secrecy rate so that the users in the wireless communication network can transmit data securely at a reasonably high speed. In this research, we first propose the coding technique, which can improve the efficiency of bandwidth utilization. Second, we propose the positioning-aided cooperative communication, which also can maximize the efficiency of bandwidth utilization. Third, we propose the optimization framework to maximize the secrecy rate of wireless communication networks under the constraint that the receivers do not have their own energy source.

Project Code : MRG5680177

Project Title : Wireless Network Coding for Cooperative Indoor Positioning in Cognitive Radio Networks

Investigator : Assistant Professor Dr. Kampol Woradit, Srinakharinwirot University

E-mail Address : w_kampol@hotmail.com

Project Period : June 2013 – August 2020

Keywords : Cooperative communications, cognitive radios, physical secrecy, wireless power transfer

Objectives

1. Building optimization framework for wireless communication networks using orthogonal-frequency division-multiple access with coding to maximize the secrecy rate subject to the constraint that the receivers do not have their own energy source, where the optimizers are subcarrier allocation and power splitting ratios.

2. Developing protocol and algorithm that yield the optimality with the reasonable complexity

3. Writing computer simulation program to observe the results to gain insights about the limitation of wireless communication networks in terms of secrecy rate.

Methods

Cognitive radios

Due to the scarcity of the frequency spectrum, [S. Haykin[1]] suggested that when a user who hold frequency license does not make a transmission especially the case that the data traffic is not saturated, the frequency spectrum becomes unused, and other user who does not hold the frequency license can make a transmission using that frequency during that time interval without the frequency license, and the user who hold the frequency license will not notice nor be affected by the transmission. The user who hold the frequency band is referred to as 'primary user' and another user is referred to as 'secondary user'. This scheme works well as long as the secondary user ensure that the transmission will take place only during the time interval that the primary user does not make a transmission. To do that, the secondary user needs to sense the transmission of the primary user by detecting the energy in that frequency, where many research papers investigated the sensing such as [Y. Liang[2]]. In practice, where noise and fading exist in radio frequency environment, sensing is not perfectly correct, and has two types of errors: detection error and false alarm, which must be minimized. As a result, there is a chance that the secondary user mistakenly makes a transmission while the primary user is transmitting, or the secondary user misses the chance to make a transmission when the primary user does not transmit.

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," IEEE J. Select. Areas Commun., vol. 23, no. 2, pp. 201-220, Feb. 2005.

[2] Y. Liang, Y. Zeng, E. C. Y. Peh and A. T. Hoang, "Sensing-Throughput Tradeoff for Cognitive Radio Networks," in *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326-1337, April 2008.

Even though this scheme realizes the *orthogonal* multiple access between the primary user and the secondary user by opportunistic time division, this scheme will be feasible unless the data traffic of the primary user is saturated. Otherwise, the primary user will occupy the frequency all the time, and there will be no time interval that the secondary user can transmit. In such case, the orthogonal multiple access cannot be realized. Nevertheless, the Federal Communications Commission (FCC) allows the secondary user to make a transmission while the primary user is transmitting if the interference level is not greater than a limit [FCC[3]], which means the *non-orthogonal* multiple access in power domain is allowed. Hence, the secondary user can also transmit during the time interval that the primary user transmits if the secondary user transmits with a power that causes an interference less than the regulated level to the primary user. The primary user will regard the interference from the secondary user as a noise, where the signal-to-noise ratio of the primary user turns into signal-to-interference-plus-noise ratio, which degrades the communication link of the primary user, where the degradation is acceptably small. For example, as shown in Fig. 1, let $h_{P,P}$ denote the channel coefficient between the primary user transmitter and the primary user receiver. Let $h_{S,P}$ denote the channel coefficient between the primary user transmitter and the secondary user receiver. let $h_{S,S}$ denote the channel coefficient between the secondary user transmitter and the secondary user receiver. let $h_{P,S}$ denote the channel coefficient between the secondary user transmitter and the primary user receiver.

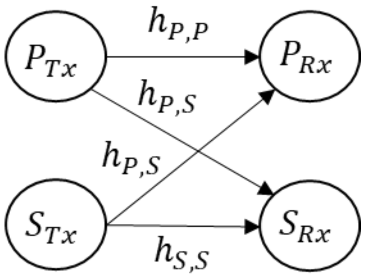


Fig. 1 Cognitive radios model

The signal-to-noise ratio of the primary user without secondary user is given by

$$SNR_{PU} = \frac{\left|< h_{P,S}, h_{P,P} >\right|^2}{\left\|h_{P,P}\right\|^2}$$

[3] FCC, “ET Docket No 03-327 Notice of inquiry and notice of proposed rulemaking,” Nov. 2003.

while the signal-to-interference-plus-noise ratio is given by

$$SINR_{PU} = \frac{\left\|h_{P,P}\right\|^2 P_P}{\frac{\left|< h_{P,S} h_{P,P} >\right|^2}{\left\|h_{P,P}\right\|^2} P_S + N_0}$$

The FCC allows the secondary user to cause an interference at the primary user as long as the degradation in signal-to-noise ratio to signal-to-interference-plus-noise ratio is not greater than a threshold, which means that

$$SNR_{PU}[dB] - SINR_{PU}[dB] \leq \gamma_{threshold}[dB]$$

where the unit is in decibel.

In this scheme, notice that the secondary does not need to sense the transmission of the primary user to seek the valid time interval, but needs to ensure that the transmit power is not so high that the primary user experiences an interference above the regulated level. To do that, as the first approach, the secondary user must estimate the channel state information between itself and the primary user receiver based on the reciprocity, when the primary user receiver turns to transmit, and uses that channel state information to calculate its maximum transmit power that creates interference less than the allowed level at the primary user receiver. This approach is transparent to the primary user.

As the second approach, both the primary user receiver and the secondary user receiver are deployed with multiple antennas, and the primary user is upgraded to accommodate the existence of a secondary user. So, this approach is not transparent to the primary user. The primary user must be able to estimate the channel state information between the secondary user transmitter and the primary user receiver by feeding the channel state information estimated at the primary user receiver back to the primary user transmitter. Based on the estimated channel state information and the knowledge of the transmit power of secondary user, the primary user calculates the amount of degradation from the signal-to-noise ratio to the signal-to-interference-plus-noise ratio. If the amount of degradation is greater than an allowed level, the primary user will signal the secondary user not to transmit and vice versa. In case that the transmit power of the secondary user is adjustable, the primary user will signal the secondary user the allowed transmit power. This approach is extended to the case that there are more than one secondary user, and is referred to as the opportunistic spatial orthogonalization [C. Shen[4]]. When there are several secondary users, the primary user needs to estimate the channel state information between every secondary user transmitter and the primary user receiver, which increases the workload of the primary user, but more secondary users are beneficial as follows. The primary user calculates the interference level created by each secondary user at the primary user receiver based on the known channel state information, and considers only the secondary user that creates the minimum interference level whether to allow the transmission at that secondary user or not. Since all channel state are independent, more secondary users create the diversity that increase the probability that a secondary user is eligible to transmit or increase the transmit power.

It can be seen that this work assumes that primary user knows many channel state information and controllability over secondary users while secondary users do not know channel state information of other nodes. However, primary user should be an existing system and the introduction of secondary user should be transparent to primary user, which should not know many channel state information and should not be able to control secondary users. Also, secondary users should know the channel state information of the link from primary user, because secondary user is supposed to be cognitive and know the pilot protocol of primary user. So, precoding at secondary user to avoid interference at primary user is feasible. Another assumption is that primary user's arrival rate is saturated. We think secondary user might have a finite arrival rate. Eventually, that work actually proposes the non-orthogonal scheme, which requires a certain level of interference tolerance at primary user.

Half-orthogonal transimssion

Single primary user and single secondary user case: we assume that the secondary user transmitter knows channel state information of primary user and secondary user receiver. Secondary user transmitter needs at least 3 antennas, so that it can use two null bases to cancel the projection of its eigen basis on the eigen basis of PU. The reason that it needs two null bases is that the channel coefficients are complex numbers which have both real part and imaginary part, and two weights are needed for cancelling both parts.

[4] C. Shen and M. P. Fitz, "Dynamic spatial spectrum access with opportunistic orthogonalization," in *Proceedings of the 43rd Conference on Information Sciences and Systems (CISS)*, Mar. 18-20, 2009, pp. 600—605.

Single primary user and N secondary users case: All secondary users need to cooperate each other to let an secondary transmitter knows the channel state information of all other secondary users in addition to the channel state information of the primary user. All secondary users need to establish a media access control protocol so that only one secondary user transmits at one time. Also, every secondary must have at least 2N+1 antennas because it needs 2N null bases to cancel the projection of the transmitting SU on the eigen basis of primary user as well as eigen bases of N-1 other secondary users, where these N projections have both real part and imaginary part. So, considering every increasing secondary user, a secondary user needs two more antennas.

Scalability

Even though we can add two antennas at every secondary user transmitter for every added secondary user, every secondary user has to normalize the linear combination of bases to obtain a unit precoding. When more bases are combined, the normalization is likely to make the weight of the eigen basis of the transmitting secondary user smaller. Note that the weight will be much smaller if the projection of the eigen basis of secondary user on the eigen basis of primary user or on the eigen basis of any other secondary user is large. As a result, the instantaneous transmission rate of the transmitting secondary user might be low. The media access control protocol of secondary users should let the secondary user having maximum instantaneous transmission rate to transmit. It is interesting to observe the trend of average transmission rate among all secondary users as a function of number of secondary users.

Network and Channel Models

We consider a base station communicating in downlink with K user nodes as illustrated in Fig. 2. The base station has M antennas, which are used to do precoding, and each user node has a single antenna. The base station uses OFDMA with N subcarriers, which are allocated to all users. Each subcarrier must be allocated to only one user. The subcarrier allocation is one of the two optimizers to be optimized by the proposed algorithm.

The base station has K streams of data bits to transmit to K user nodes. Each data bit stream is encoded separately, and is then modulated into constellation symbols, where the channel coding and modulation are abstracted here due to the scope of this paper. Every stream of constellation symbols waits in a first-in first-out (FIFO) buffer to be transmitted to each user node. Let $k \in \{1,2,3,\ldots,K\}$, denote the index of user node. Consider an OFDMA symbol which contains N subcarriers. Suppose 3 subcarriers, namely the 2nd, the 3rd and the 5th subcarriers, are allocated to the k^{th} user node. Three consecutive constellation symbols of the k^{th} user node leave the buffer, and are mapped onto the 2nd, the 3rd and the 5th subcarriers. Let c_n denote the constellation symbol to be transmitted via the n^{th} subcarrier, where $\mathbb{E}[|c_n|^2] = 1$.

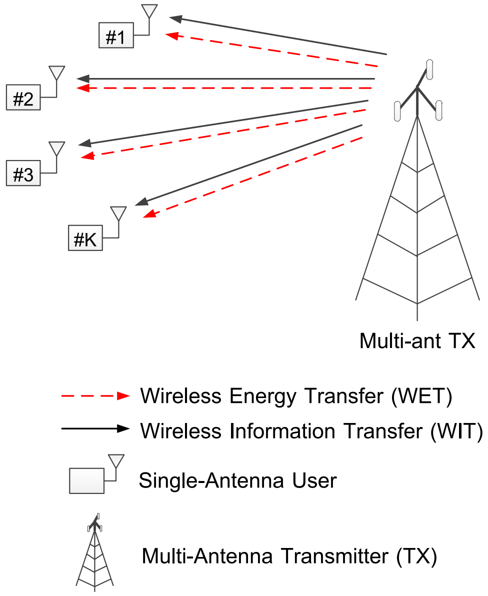

#1
#2
#3
#K
Multi-ant TX
Wireless Energy Transfer (WET)
Wireless Information Transfer (WIT)
Single-Antenna User
Multi-Antenna Transmitter (TX)

Fig. 2 Network Model

The constellation symbol at each subcarrier is processed by precoding into M signals to be transmitted with M antennas. The base station modulates a signal $S_{m,n}$ with the n^{th} subcarrier at the m^{th} antenna, where n $\in \{1,2,3,\ldots,N\}$ and m $\in \{1,2,3,\ldots,M\}$. Within an OFDMA symbol, the Inverse Fast Fourier Transform (IFFT) gives the modulated signal $s_{m,t}$ at the m^{th} antenna and the t^{th} sampling time as

$$s_{m,t} = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} S_{m,n} e^{j2\pi(n-1)(t-1)/N} \quad ,$$

where $t \in \{1,2,3,\ldots,N\}$.

The channel is assumed to be quasi-static, which means all channel coefficients are constant during an OFDMA symbol, and each channel coefficient changes independently in the next OFDMA symbol. The channel coefficients are modeled by frequency-selective Rayleigh fading, where the power delay profile have L taps. Since the base station has M antennas and every user node has a single antenna, there are MKL channel coefficients. Let $h_{m,k,l}$ denote the channel coefficient between the mth antenna and the kth user node at the lth tap, where m ∈ $\{1,2,3,\ldots,M\}$, k ∈ $\{1,2,3,\ldots,K\}$, l ∈ $\{1,2,3,\ldots,L\}$. The channel coefficient $h_{m,k,l}$ is circularly symmetric complex Gaussian random variable with zero mean and variance δ_l^2, and can be written as

$$h_{m,k,l} \sim \mathcal{CN}\left(0, \delta_l^2\right)$$

where

$$\sum_{l=1}^{L} \delta_l^2 = 1$$

for normalization.

The channel frequency response at the nth subcarrier between the mth antenna of the base station and the kth user can be expressed as

$$H_{m,k,n} = \frac{1}{\sqrt{N}} \sum_{l=1}^{L} h_{m,k,l} e^{-j2\pi(l-1)(n-1)/N}$$

It is assumed that the base station perfectly knows the channel frequency response of every subcarrier and of every user, and uses the channel knowledge to do precoding for maximum channel gain in each subcarrier. More specifically, suppose the nth subcarrier is allocated to the kth user. The base station does precoding to the kth user at the nth subcarrier by using singular value decomposition as follows. We define the vector $\boldsymbol{H}_{k,n} = \left[H_{1,k,n}, H_{2,k,n}, H_{3,k,n}, \ldots, H_{M,k,n}\right]^T$ as the channel frequency response of all links from M base station antennas to the kth user at the nth subcarrier. The singular value decomposition of $\boldsymbol{H}_{k,n}$ gives the vector $\boldsymbol{H}_{k,n}/\left|\boldsymbol{H}_{k,n}\right|_2$ as the first column of the M x M unitary matrix. Suppose the constellation symbol to be transmitted at the nth subcarrier is c$_n$. Then, the signal S$_{m,n}$ is given by

$$S_{m,n} = \frac{\overline{H}_{m,k,n}}{||\boldsymbol{H}_{k,n}||_2} c_n$$

where m $\in \{1,2,3,\ldots,\mathrm{M}\}$. The channel gain can be calculated from the channel frequency response equation and the beamforming equation for the nth subcarrier, which is allocated to the kth user in this example.

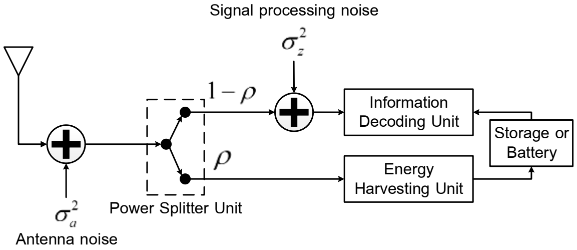


Fig. 3 SWIPT scheme with power splitting at a receiver

The signals S$_{m,n}$ in the beamforming equation are separately modulated into M baseband OFDMA signals for each antenna as shown in the inverse fast Fourier transform equation. Each baseband OFDMA signal is modulated into radio frequency signal to be transmitted with each antenna. The transmitted radio frequency signals propagating from M base station antennas through L-tap channels with the channel coefficients described in the channel coefficient distribution equation are combined at the receive antenna of each user node.

All user nodes do not have their own power supply, and rely on energy harvesting. The energy harvesting scheme is SWIPT as shown in Fig. 3. Each user is able to split the received radio frequency signals into two parts. One part is for energy harvesting, and another part is fed to the demodulator, which converts the radio signals into baseband OFDMA signal and then computes the Fast Fourier Transform (FFT). At the kth user node, the ratio between the powers of the two parts is determined by the power splitting ratio ρ_k, where $\rho_k \in [0,1]$ for k $\in$ $[1,2,3,\ldots,\mathrm{K}]$. Considering the energy of the received signals at the kth user node, a portion of ρ_k is used for powering the receiver, and a remaining portion of 1-ρ_k is used for information demodulation and decoding.

Suppose the conversion efficiency of energy harvesting at each receiver is η, where $0 \leq \eta \leq 1$. The total harvested energy at the kth user node is obtained by

$$E_k = \eta\rho_k \frac{P_t}{NM} \sum_{n=1}^{N} \sum_{m=1}^{M} |S_{m,n} H_{m,k,n}|^2 + \sigma^2$$

where P$_t$ denotes the transmit power of the base station and σ^2 denotes the variance of additive white Gaussian noise contributed from both the antenna noise with variance σ_a^2 and the processing noise with variance σ_z^2. Here, σ^2 is assumed to be identical for every user node. Note that the noise is disadvantageous to demodulation and decoding but becomes beneficial for energy harvesting. A user node needs to harvest energy not less than the minimum amount of energy sufficient to receive information. This minimum required energy is the same for all user nodes and is denoted by $\tilde{E}$.

Given that the nth subcarrier is allocated to the kth user, the instantaneous rate of the k'th user at the nth subcarrier is denoted by R$_{k',n}$ and can be expressed as

$$R_{k,n} = \log_2 \left(1 + \frac{P_t(1-\rho_k)}{NM\sigma^2} \sum_{m=1}^{M} |H_{m,k,n}|^2 \right),$$

when k'=k, and

$$R_{k',n} = \log_2 \left(1 + \frac{P_t(1-\rho'_k)}{NM\sigma^2} \left| \sum_{m=1}^{M} \frac{\overline{H}_{m,k,n}}{\|\boldsymbol{H}_{k,n}\|_2} H_{m,k',n} \right|^2 \right)$$

when k' ≠ k.

In the literature, an eavesdropper is usually a node which is not a user of the network. In this paper, all users can eavesdrop each other. When the base station transmits an information to the kth user via the nth subcarrier, the users other than the kth user can attempt to decode the information in the nth subcarrier. To achieve secrecy, the base station cannot transmit the information at the rate in the instantaneous rate equation and have to transmit the information at the secrecy rate instead. The secrecy rate of the kth user at the nth subcarrier is defined as the difference between the instantaneous rate of the kth user and the maximum instantaneous rate among all other users and can be written as

$$R_{k,n}^{+} = \left(R_{k,n} - \max_{k' \neq k} R_{k',n} \right)^{+}$$

where $(\cdot)^{+} \triangleq \max\{\cdot, 0\}$. The secrecy rate of the kth user depends on all subcarriers allocated to the kth user. Hence, we define the indicator variable denoted by $x_{k,n}$ as

$$x_{k,n} = \begin{cases} 1, & \text{if } n^{th} \text{ subcarrier is allocated to } k^{th} \text{ user} \\ 0, & \text{otherwise} \end{cases} .$$

Then, the secrecy rate of the kth user is $\sum_{n=1}^{N} x_{k,n} R_{k,n}^{+}$. If the objective is to maximize the average secrecy rate among all user nodes, the base station will allocate the subcarriers and adjust the splitting ratios of all user nodes in such a way that most user nodes obtain zero secrecy rate, which is not fair. This paper uses the max-min fairness criterion to achieve fairness. Accordingly, we maximize the secrecy rate of the user node that obtains the minimum secrecy rate among all user nodes. The secrecy rate of the user node having the minimum secrecy rate among all users is denoted by R^{+} and is defined as

$$R^{+} = \min_{k} \sum_{n=1}^{N} x_{k,n} R_{k,n}^{+}$$

Our objective is to maximize R^{+}.

Algorithm

Based on the assumption described in the described model, the base station has the perfect knowledge of all channel coefficients with the objective to maximize the secrecy rate R^+ by optimizing two variable sets:

- the subcarrier allocation x_{k,n}, k \in \{1,2,3,...,K\}, n \in \{1,2,3,...,N\}
- the power splitting ratio \rho_k, k \in \{1,2,3,...,K\}

under four constraints as follows.

- Each subcarrier can be allocated to only one user.
- The power splitting ratio must not be negative.
- The power splitting ratio must not be greater than 1.
- The energy harvested at every user node must not be less than \tilde{E}, which is the minimum required energy to receive the information from the base station.

Accordingly, the optimization problem can be formulated as

$$
\begin{aligned}
\underset{\boldsymbol{x},\boldsymbol{\rho}}{\text{maximize}} \quad & R^+ \\
\text{subject to} \quad & \sum_{k=1}^{K} x_{k,n} \le 1, && \forall n, \\
& x_{k,n} \in \{0,1\}, && \forall k, \forall n, \\
& \rho_k \ge 0, && \forall k, \\
& \rho_k \le 1, && \forall k, \\
& E_k \ge \tilde{E}, && \forall k,
\end{aligned}
$$

where x denotes the vector of indicator variables x_{k,n}, k\in\{1,2,3,...,K\}, n\in\{1,2,3,...,N\} and rho denotes the vector of power splitting ratios rho_k, k\in\{1,2,3,...,K\}. The constraint of unique x does not allow the base station to allocate any subcarrier to more than one user nodes. The constraints of lower bound and of upper bound present the fact that every user node solely relies on the energy harvested from the received signals. The constraint of energy imposes the minimum harvested energy requirement of every user node for receiving information from the base station.

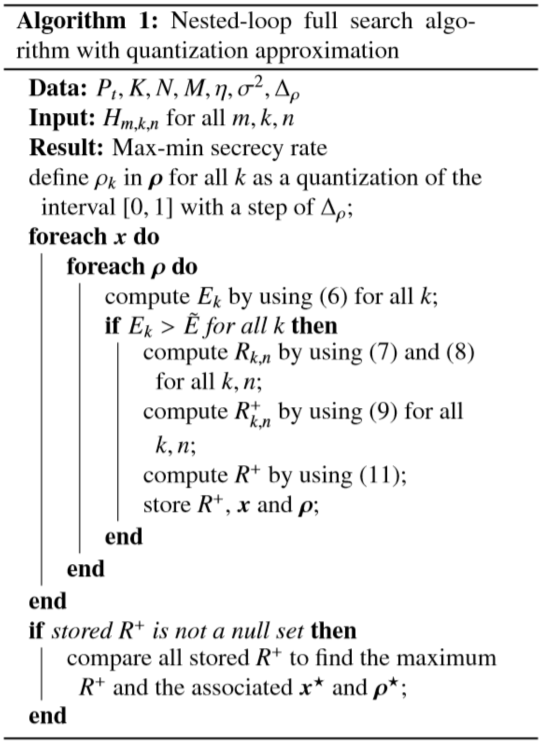
From the total harvested energy equation, when channels associating with the k^{th} user node experience fading, \rho_k must be increased to meet the requirement of constraint of energy. With deep faded channels, it is sometimes possible that the constraint of energy is contradicted even when \rho_k reaches 1. Due to the constraint of upper bound, \rho_k cannot be increased further. In that case, there is no feasible solution and the outage occurs, which means the base station does not transmit information to the user node and the whole system has zero secrecy rate. According to the assumption that the channels are quasi-static, the base station waits until deep fading is over to transmit the next OFDMA symbol.

The objective function in objective function is not convex, hence the optimization problem is also not convex. To avoid the locally optimal solutions, the solution should be sought by full search. The vector of indicator variables \boldsymbol{x} has a finite feasible set under the constraints of unique x and of possible x, thus it is straightforward to conduct a full search on \boldsymbol{x}. On the other hand, a power splitting ratio \rho_k is a continuous variable, thus the vector of power splitting ratios \boldsymbol{\rho} has an infinite feasible set. In addition, the vector of indicator variables \boldsymbol{x} and the vector of power splitting ratios \boldsymbol{\rho} are involved in objective function and the energy constraint, thus both vectors cannot be separately searched.

To obtain the solution as close to the globally optimal solution as possible, the search is done in nested loops composed of the outer loop and the inner loop. The outer loop tries every possible vector of indicator variables \boldsymbol{x}. Considering (\ref{eq:uniquexconstraint}) and (\ref{eq:xsetconstraint}), the outer loop has K^N different values to search. The inner loop tries possible vectors of power splitting ratios \boldsymbol{\rho}. The vector components \rho_k, k\in\{1,2,3,...,K\}, are continuous variables, where the full search cannot be conducted. Considering (\ref{eq:rholowerbound}) and (\ref{eq:rhoupperbound}), however, every power splitting ratio \rho_k is a number between 0 and 1, and thus can be quantized into a finite set of values to search. Relaxing the full search by quantizing the power splitting ratios can give the result as close to that of the full search as possible by reducing the quantization step size until the search complexity limitation is reached. Considering a quantization step size of \Delta_\rho and K user nodes, the inner loop has \left\lceil 1/\Delta_\rho \right\rceil^K different values to search.

In the inner loop, \boldsymbol{x} and \boldsymbol{\rho} are constants and the harvested energy of every user node E_k is calculated by using the total harvested energy. Then, E_k is compared with the minimum harvested energy requirement \tilde{E} according to the constraint of energy. If any user node does not satisfy the constraint of energy, \boldsymbol{x} and \boldsymbol{\rho} of that loop are not feasible and the search moves on to the next loop. In case that all loops including both outer and inner loops are not feasible, an outage occurs and the secrecy rate is not defined for that realization of channel coefficients. The base station and all user nodes wait until the next OFDMA symbol (a new realization of channel coefficients) without any transmission.

For the inner loop that \boldsymbol{x} and \boldsymbol{\rho} are feasible, the instantaneous rates of all user nodes at all subcarriers R_{k,n} are calculated by substituting \boldsymbol{\rho} in the first instantaneous rate equation and the second instantaneous rate equation, and are substituted in secrecy rate equation to calculate the secrecy rate of all user nodes R_{k,n}^+. The secrecy rate of all user nodes are substituted in the minimum secrecy rate to obtain the objective value which is the secrecy rate of the user node having the minimum secrecy rate among all users R^+. The obtained objective values from all loops including both outer and inner loops are compared to find the loop that gives the maximum objective value R^+ according to objective function, and the \boldsymbol{x} and \boldsymbol{\rho} of that loop are the search result which is the optimization solution, and are denoted by \boldsymbol{x}^\star and \boldsymbol{\rho}^\star. The proposed algorithm can be summarized as shown in the algorithm below.



Algorithm 1: Nested-loop full search algorithm with quantization approximation

```
Data: $P_t, K, N, M, \eta, \sigma^2, \Delta_\rho$
Input: $H_{m,k,n}$ for all $m, k, n$
Result: Max-min secrecy rate
define $\rho_k$ in $\boldsymbol{\rho}$ for all $k$ as a quantization of the
  interval [0, 1] with a step of $\Delta_\rho$;
foreach $\boldsymbol{x}$ do
    foreach $\boldsymbol{\rho}$ do
        compute $E_k$ by using (6) for all $k$;
        if $E_k > \tilde{E}$ for all $k$ then
            compute $R_{k,n}$ by using (7) and (8)
              for all $k, n$;
            compute $R^+_{k,n}$ by using (9) for all
              $k, n$;
            compute $R^+$ by using (11);
            store $R^+$, $\boldsymbol{x}$ and $\boldsymbol{\rho}$;
        end
    end
end
if stored $R^+$ is not a null set then
    compare all stored $R^+$ to find the maximum
      $R^+$ and the associated $\boldsymbol{x}^\star$ and $\boldsymbol{\rho}^\star$;
end
```

Coding System

We consider an SF coding system, which employs M_T transmit antennas, M_R receive antennas, N subcarriers, and operates in a frequency-selective Rayleigh fading channel that results from power delay profile with M_L taps between each pair of transmit and receive antennas as shown in Fig. 4. The transmitter is equipped with an SF encoder that accepts a data input, and outputs a two-dimensional array of symbols as an SF codeword to be transmitted over M_T transmit antennas, and N subcarriers. Each SF codeword can be expressed as an $N \times M_T$ matrix,

$$C = \begin{bmatrix} c_1^1 & c_1^2 & \cdots & c_1^{M_T} \\ c_2^1 & c_2^2 & \cdots & c_2^{M_T} \\ \vdots & \vdots & \ddots & \vdots \\ c_N^1 & c_N^2 & \cdots & c_N^{M_T} \end{bmatrix}$$

where $c_n^{m_T}$ denotes the symbol transmitted over the n^{th} subcarrier by the $m_T{}^{\text{th}}$ transmit antenna. Each transmit antenna corresponds to an OFDM transmitter that applies an N-point inverse fast Fourier transform (IFFT) to each column of the matrix C and attaches a cyclic prefix. The OFDM symbols are transmitted from all transmit antennas simultaneously and synchronously. The symbol received at each receive antenna is corrupted by additive white Gaussian noise and the multiplicative multipath fading. At the receiver end, after matched filtering, removing the cyclic prefix, and applying fast Fourier transform (FFT), the received symbol at the n^{th} subcarrier at the $m_R{}^{\text{th}}$ receive antenna is given by

$$y_n^{m_R} = \sqrt{\frac{\rho}{M_T}} \sum_{m_T=1}^{M_T} c_n^{m_T} H_n^{m_T,m_R} + z_n^{m_R}$$

where

$$H_n^{m_T,m_R} = \sum_{l=1}^{M_L} h_l^{m_T,m_R} e^{-j2\pi n \tau_l / N}$$

is the channel frequency response at the n th subcarrier between the m_T th transmit antenna and the m_R th receive antenna. The τ_l is the delay of the l th tap which is assumed to be identical for all pair of transmit and receive antennas. The $h_l^{m_T,m_R}$ is the complex fading coefficient between the m_T th transmit antenna and the m_R th receive antenna, and is modeled as zero-mean complex Gaussian random variables with variance δ_l^2 which is also assumed to be identical for all pairs of transmit and receive antennas. The variances of all taps are normalized such that

$$\sum_{l=1}^{M_L} \delta_l^2 = 1$$

The $z_n^{m_R}$ denotes the additive complex Gaussian noise with zero mean and unit variance at the n th subcarrier at the m_R th receive antenna. The factor ρ is the average SNR at each receive antenna.

At the receiver, the Viterbi algorithm is applied for the decoding of SF codes with an assumption that the channel state information is perfectly known. The metric of each trellis path, associated with a codeword C, is given by

$$\sum_{n=1}^{N} \sum_{m_R=1}^{M_R} \left| y_n^{m_R} - \sum_{m_T=1}^{M_T} c_n^{m_T} H_n^{m_T,m_R} \right|^2$$

Finally, the codeword $\tilde{C}$, associated with the trellis path with the lowest metric, are decided to be the received codeword, and the codeword can be mapped into the decoded data. The error occurs when the received codeword $\tilde{C}$ differs from the transmit codeword C.

The design criteria for SF codes under frequency-selective Rayleigh fading environments are well established, which include the diversity (rank) criterion and the product criterion. The diversity criterion provides a framework that aims to maximize diversity advantage, whereas the product criterion helps ensure high coding gain. For convenience, these criteria will be concisely summarized here.

Given the frequency spacing between adjacent subcarriers is Δf and using the notation $w = \exp\left(-j2\pi\Delta f/N\right)$, we have

$$W = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ w^{\tau_1} & w^{\tau_2} & \cdots & w^{\tau_{M_L}} \\ \vdots & \vdots & \ddots & \vdots \\ w^{(N-1)\tau_1} & w^{(N-1)\tau_2} & \cdots & w^{(N-1)\tau_{M_L}} \end{bmatrix}$$

and

$$R = Wdiag(\delta_1^2, \delta_2^2, \dots, \delta_{M_L}^2)W^H$$

Defining the matrix Δ as

$$\Delta \triangleq \left(C - \tilde{C}\right)\left(C - \tilde{C}\right)^H$$

Also, let ρ be the rank of $\Delta \circ R$, and λ_1, λ_2, …, λ_ρ be the nonzero eigenvalues of $\Delta \circ R$, where $\circ$ is the Hadamard product. We can formulate the criteria as follows

- Diversity criterion: The minimum rank of $\Delta \circ R$ over all pairs of distinct SF codewords C and $\tilde{C}$ should be as large as possible
- Product criterion: The minimum value of the product $\prod_{i=1}^{\rho} \lambda_i$ over all pairs of distinct SF codewords C and $\tilde{C}$ should also be maximized.

Note that subsequent derivation based on the diversity criterion leads to an interesting conclusion that the maximum achievable diversity is at most $\min\left\{M_L M_T M_R, NM_R\right\}$ [10]. This makes SF codes different from ST codes that the diversity limit of SF codes is M_L times greater than that of ST codes, whose diversity limit is $\min\left\{M_T M_R, NM_R\right\}$ [1]. It should also be remarked that the power delay profile of channel depends on the radio environment, which can change as the user moves from one area to another area with different radio environment. Therefore, the number of taps M_L can vary with the mobility of the user. When we design an SF code, the number of taps M_L is a constant that we need to choose. It should be chosen to be an expected number of taps, found in real radio environment, so that the designed SF codes do not under-exploit the available diversity, or do not have high complexity without gaining more diversity.

Coding Design Method

In this section, we will present our proposed SF code design method for the system with M_T transmit antennas and N subcarriers. Our approach to the code design is based on trellis-coded modulation, which treats modulation and coding as an integrated entity, and the encoding can be described by a trellis diagram. To obtain the output as an SF codeword expressed by an $N \times M_T$ matrix in (1), the encoder takes the input as a series of $N/(M_T L)$ blocks of data bits, where L is a fixed number $\left(1 \le L \le M_L\right)$. The size of each block is determined by the desired spectral efficiency. That is, for the system with the spectral efficiency of $\log_2 b$ bits/subcarrier, the block size is set to $\log_2 b^{M_T L}$ bits, and thus each block of input data belongs to the set of $b^{M_T L}$ different data bit patterns. Each data bit pattern shall be denoted as D_i, $i \in \left\{1,\ldots,b^{M_T L}\right\}$. When the encoder takes a block of input data D_i, it changes the state and outputs a channel symbol matrix S_i^k with size $M_T L \times M_T$ according to the structure of the trellis diagram and the branch labeled D_i / S_i^k, where k represents the previous state of the encoder; this is illustrated in Fig. 2. After all $N/(M_T L)$ input data blocks are taken into the encoder, the complete SF codeword is obtained.

The method of constructing SF codes consists of four procedures: a) constructing the set of channel symbol matrices; b) set partitioning; c) designing the transition branches and d) labeling the transition branches. Each of these procedures will be described below.

In constructing the channel symbol matrices S_i^k, we adopt the orthogonal designs for the first step. An example of 2×2 orthogonal design, which is applicable for M_T = 2, is

$$\begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix}$$

Then for $L \ge 2$, the channel symbol matrices are constructed by concatenating row-wise L such matrices of different entries. For example, for L = 2, the concatenated orthogonal design will become

$$\begin{bmatrix} x_1 & -x_2^* & x_3 & -x_4^* \\ x_2 & x_1^* & x_4 & x_3^* \end{bmatrix}^T$$

Based on this design platform, the next step is to find the set of P channel symbol matrices by mapping appropriate constellation points to x_1, x_2, x_3, x_4. Henceforth, we will represent the constellation points corresponding to the channel symbol index p where $p \in \{1,...,P\}$ by $x_1(p)$, $x_2(p)$, $x_3(p)$, $x_4(p)$. For convenience, we will also define a vector $\mathbf{x}(p) = \left[x_1(p) \quad x_2(p) \quad x_3(p) \quad x_4(p)\right]^T$. To maximize the diversity advantage and achieve high coding gain, constellation points should be mapped such that the following two constraints are satisfied.

$$\|\mathbf{x}(p)\mathbf{x}^H(p)\|^2 = M_T L, p \in \{1, \dots, P\},$$

and

$$min\|\mathbf{x}(p) - \mathbf{x}(\tilde{p})\|^2, \text{ for } p, \tilde{p} \in \{1, \dots, P\}, p \neq \tilde{p},$$

is maximized. Note that the proofs of these constraints will be given in Proposition I and Corollary I at the end of this subsection. Since finding such a mapping through exhaustive search is cumbersome if not impossible, we introduce a mapping that not only conforms to the two constraints but also requires much less searching complexity as follows:

$$\mathbf{x}(p) = \frac{1}{\sqrt{M_T}}\begin{bmatrix} exp\big(j2\pi\big(q_1(p-1)(mod \quad P)\big)/P\big) \\ exp\big(j2\pi\big(q_2(p-1)(mod \quad P)\big)/P\big) \\ exp\big(j2\pi\big(q_3(p-1)(mod \quad P)\big)/P\big) \\ exp\big(j2\pi\big(q_4(p-1)(mod \quad P)\big)/P\big) \end{bmatrix}, \quad p \in \{1, \dots, P\}$$

where q_1, q_2, q_3 and q_4 are odd numbers between 1 and $P-1$, and are chosen to maximize (12). The benefits of using (13) are 2-fold. First, the requirement in (12) is satisfied with any $q_1, \dots, q_4$. Second, searching for the $q_1, \dots, q_4$ that maximize (12) is not tedious. Considering the fixed $q_1, \dots,$ q_4, the minimum value in (12) can be obtained by varying only $\tilde{p}$ and fixing p. For example, fixing p = 1, it is reduced to

$$min\|\mathbf{x}(1)-\mathbf{x}(\tilde{p})\|^2 \text{, for } \tilde{p}\in\{2,\ldots,P\},$$

which turns the ${}^{P}\mathrm{C}_2$ comparisons to $P-1$ comparisons. Also, searching for $q_1,\ldots,q_4$, is reduced from $(P/2)^4$ cases to $\sum_{g=0}^{M_TL-1} {}^{M_TL-1}\mathrm{C}_g \, {}^{P/2}\mathrm{C}_{g+1}$ cases, because interleaving $q_1,\ldots,q_4$ does not effect the Euclidean distance $\|\mathbf{x}(p)-\mathbf{x}(\tilde{p})\|$. For example, at P = 16, we search $q_1,\ldots,q_4$ for 330 cases instead of 4096 cases (the searched result is 1,3,5,9).

The proofs that the constructed channel symbol matrix set guarantee obtaining the maximum diversity and high coding advantage are given as follows.

Proposition 1: Using the constructed channel symbol matrix set to design an SF trellis code, the minimum rank of $\Delta\circ R$ over all pairs of distinct SF codewords C and $\tilde{C}$ is maximized.

Proof: Consider the potential pairs of C and $\tilde{C}$ that give the minimum rank of $\Delta\circ R$. They are the pairs that are different for only one sub-SF codeword. Since the structure of the trellis diagram is identical for all blocks of input data, we consider only the pairs that are different at the first sub-SF codeword. Using the concatenated orthogonal design, the Δ is given by

$$\begin{bmatrix} \alpha\mathbf{I}_{M_T}\otimes\mathbf{I}_L & \mathbf{0}_{(M_TL)\times(N-M_TL)} \\ \mathbf{0}_{(N-M_TL)\times M_TL} & \mathbf{0}_{(N-M_TL)\times(N-M_TL)} \end{bmatrix}$$

where α is a scalar, $\mathbf{I}$ and $\mathbf{0}$ are identity matrix and zero matrix, respectively. The minimum rank of $\Delta\circ R$ equals the minimum rank of

$$(\mathbf{I}_{M_T}\otimes\mathbf{I}_L)\circ(\widetilde{W}diag(\delta_1^2,\delta_2^2,\ldots,\delta_{M_L}^2)\widetilde{W}^H),$$

where

$$\widetilde{W} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ w^{\tau_1} & w^{\tau_2} & \cdots & w^{\tau_{M_L}} \\ \vdots & \vdots & \ddots & \vdots \\ w^{(M_T L-1)\tau_1} & w^{(M_T L-1)\tau_2} & \cdots & w^{(M_T L-1)\tau_{M_L}} \end{bmatrix}$$

The matrix $(\mathbf{I}_{M_T} \otimes \mathbf{I}_L)$ in (16) is not a full-rank matrix because the first M_T rows repeat for L times. After taking the Hadamard product, the repeated rows become

$$\begin{bmatrix} \sum_{l=1}^{M_L} \delta_l^2 \, exp\left(\frac{j2\pi(l-1)(1-f)}{N}\right) \\ \sum_{l=1}^{M_L} \delta_l^2 \, exp\left(\frac{j2\pi(l-1)(M_T-f)}{N}\right) \\ \vdots \\ \sum_{l=1}^{M_L} \delta_l^2 \, exp\left(\frac{j2\pi(l-1)((L-1)M_T-f)}{N}\right) \end{bmatrix}^T \otimes \begin{bmatrix} 1 \\ \mathbf{0}_{M_T \times 1} \end{bmatrix}^T$$

where $f \in \{ f_0+1, f_0+M_T, \ldots f_0+(L-1)M_T \}$ is the row index, and $f_0 \in \{1,\ldots,M_T\}$. For each f_0, all L rows are independent because all entries in these rows are the linear combinations of M_L-exponential basis, where $M_L \geq L$. Therefore, the product in (16) results in a full-rank matrix, and the minimum rank of $\Delta \circ R$ is maximized. Q.E.D.

Corollary 1: Using the constructed channel symbol matrix set to design an SF trellis code with full-rank $\Delta \circ R$, the minimum value of the product $\prod_{i=1}^{\rho} \lambda_i$ over all pairs of distinct SF codewords C and $\tilde{C}$ is maximized.

Proof: The minimum value of the product $\prod_{i=1}^{\rho} \lambda_i$ equals the minimum value of the product of nonzero eigenvalues of

$$\alpha(\mathbf{I}_{M_T} \otimes \mathbf{I}_L) \circ (\widetilde{W} diag(\delta_1^2, \delta_2^2, \ldots, \delta_{M_L}^2)\widetilde{W}^H)$$

The term $\tilde{W}diag(\delta_1^2,\delta_2^2,\ldots,\delta_{M_L}^2)\tilde{W}^H$ is determined by the channel condition, and $\mathbf{I}_{M_T}\otimes\mathbf{I}_L$ is constant. α is a scalar that is proportional to the squared Euclidean distance. Since the minimum squared Euclidean distance is maximized, the minimum α is maximized. Therefore, the product is maximized. Q.E.D.

The set partitioning used in this paper resembles the conventional one for the single antenna case. The entire set of the channel symbol matrices is partitioned into 2 sets in the first level, and each of them is partitioned again into 2 sets in the second level, and so on. In the single antenna case, the partitioning is done such that the minimum Euclidean distance product between two members within a partitioned set is maximized. This concept can be extended to our code design straightforwardly; that is to maximize the minimum value of the product of nonzero eigenvalues between two members within a partitioned set. Due to Corollary 1, maximizing this product is equivalent to maximizing the minimum value of the squared Euclidean distance, and thus, we achieve reduction in computational complexity.

For illustration purpose, we present details of set partitioning for the channel symbol matrix set example in Section III.1. Denote the entire set by $\bar{\mathbf{S}}_0=\{\mathbf{S}^1,\ldots,\mathbf{S}^{16}\}$, where $\mathbf{S}^p$ is the orthogonal design in (10), whose entries are identified by $\mathbf{x}(p)$ in (13). In the first level, the set $\bar{\mathbf{S}}_0$ is partitioned into the sets $\bar{\mathbf{S}}_{00}$ and $\bar{\mathbf{S}}_{01}$, where

$$\bar{\mathbf{S}}_{00}=\{\mathbf{S}^1,\mathbf{S}^3,\mathbf{S}^5,\mathbf{S}^7,\mathbf{S}^9,\mathbf{S}^{11},\mathbf{S}^{13},\mathbf{S}^{15}\}$$

and

$$\bar{\mathbf{S}}_{01}=\{\mathbf{S}^2,\mathbf{S}^4,\mathbf{S}^6,\mathbf{S}^8,\mathbf{S}^{10},\mathbf{S}^{12},\mathbf{S}^{14},\mathbf{S}^{16}\}$$

In the second level, the set $\bar{\mathbf{S}}_{00}$ is partitioned into the sets $\bar{\mathbf{S}}_{000}$ and $\bar{\mathbf{S}}_{001}$, where

$$\bar{\mathbf{S}}_{000} = \{\mathbf{S}^1, \mathbf{S}^2, \mathbf{S}^3, \mathbf{S}^8\},\ \bar{\mathbf{S}}_{001} = \{\mathbf{S}^4, \mathbf{S}^5, \mathbf{S}^6, \mathbf{S}^7\},$$

and the set $\bar{\mathrm{S}}_{01}$ is partitioned into the sets $\bar{\mathrm{S}}_{010}$ and $\bar{\mathrm{S}}_{011}$, where

$$\bar{\mathbf{S}}_{010} = \{\mathbf{S}^9, \mathbf{S}^{11}, \mathbf{S}^{12}, \mathbf{S}^{15}\},\ \bar{\mathbf{S}}_{011} = \{\mathbf{S}^{10}, \mathbf{S}^{13}, \mathbf{S}^{14}, \mathbf{S}^{16}\}.$$

Note that searching for partitioning a set with cardinality $\left|\bar{\mathrm{S}}\right|$ has ${}^{|\bar{\mathrm{S}}|}\mathrm{C}_{|\bar{\mathrm{S}}|/2}$ cases. In the example, there are ${}^{16}\mathrm{C}_8$ = 12,870 cases in the first level and $2\times{}^{8}\mathrm{C}_4$ = 140 cases in the second level. This is reasonable to do the full search. In the case of large set, the exhaustive search is infeasible. Accordingly, a partial search, such as random search, might be used instead.

Consider the arbitrary trellis diagram in Fig. 4. There are many possible ways to design its transition branches. Not all of them are efficient. Only certain designs give a good performance. As a result, a proper design rule must be applied. The following simple design rule can be employed to design the desired transition branches:

i) All trellis sections in the trellis diagram are identical.

ii) Every state has $b^{M_T L}$ emerging transition branches, and $b^{M_T L}$ merging transition branches.

iii) Denote an integer κ, where $2 \le \kappa \le K$. Every state transits to κ states, and is transited from κ states.

iv) Every transition between a pair of states has equal number of transition branches.

From i), we design the transition branches for only one trellis section, and the rest trellis sections use the same design. From ii) to iv), $b^{M_T L}$ is divisible by κ. For instance, suppose $b^{M_T L}$ = 16 and K = 4, then κ has to be either 2 or 4. Hence, there are only two transition branch designs that follow the rules.

In Fig. 2, the transition branch that emerges from state k with the input data bit pattern D_i is labeled with the channel symbol matrix S_i^k, which is selected from a member of the constructed set

$\bar{\mathbf{S}}_0$. The channel symbol matrices are assigned to the transition branches in accordance with the following rules:

i) Parallel transition branches are labeled with different channel symbol matrices belonging to the same partitioned set. The cardinality of the chosen set must equal the number of parallel branches.

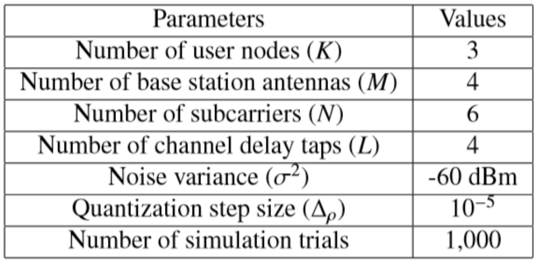
ii) All transition branches originating from one state are labeled with different channel symbol matrices belonging to the same partitioned set. The cardinality of the chosen set must equal the number of these transition branches.

iii) All partitioned channel symbol matrix set are used with equal frequency.

For example, suppose K = 2, $b^{M_T L}$ = 16 and κ = 2, then the construction of a channel symbol matrix set $\bar{\mathbf{S}}_0$ with a cardinality of 32 is required. The set $\bar{\mathbf{S}}_0$ is partitioned for two levels into $\bar{\mathbf{S}}_{000}$, $\bar{\mathbf{S}}_{001}$, $\bar{\mathbf{S}}_{010}$ and $\bar{\mathbf{S}}_{011}$, which are assigned to $\left\{S_1^1,\ldots,S_8^1\right\}$, $\left\{S_9^1,\ldots,S_{16}^1\right\}$, $\left\{S_1^2,\ldots,S_8^2\right\}$ and $\left\{S_9^2,\ldots,S_{16}^2\right\}$, respectively.

Results

Table 1: Simulation parameters



Parameters	Values
Number of user nodes (K)	3
Number of base station antennas (M)	4
Number of subcarriers (N)	6
Number of channel delay taps (L)	4
Noise variance (σ^2)	-60 dBm
Quantization step size (Δ_ρ)	10^{-5}
Number of simulation trials	1,000

Now, we examine the obtained max-min secrecy rate of the multi-user MISO-OFDMA with the proposed optimization algorithm through computer simulations. The simulation parameters are shown in Table 1, where the power delay profiles of all frequency-selective fading channels are uniform. The transmit power is allocated equally to all subcarriers, and so every subcarrier has a transmit power of P_t/N. Since the obtained max-min secrecy rate varies with every realization of channel coefficients, the computer simulations were conducted with 1,000 trials to get average results. With 3 user nodes, 6 subcarriers, and a quantization step size of 10^{-5}, the outer loop and the inner loop of the proposed algorithm have 729 loops and 28,767 loops respectively. The number of inner loops is not 10^{15} because each decimal point of a power splitting ratio is searched consecutively. For example, the first decimal point has 11 different values in the set \{0, 0.1, 0.2,...,1\}, and suppose the best value is 0.2. The second decimal point has 19 different values in the set \{0.11, 0.12, 0.13,...,0.29\}, and suppose the best value is 0.27. The third decimal point has 19 different values in the set \{0.261, 0.262, 0.263,...,0.279\} and so forth until the fifth decimal point. In this case which has 3 user nodes, the number of different values to search at the first decimal point of every power splitting ratio is 11^3, and the number of different values to search at any decimal point from the second decimal point is 19^3. Hence, the total number of different power splitting ratios to search is 11^3+4(19^3) = 28,767.

Figure 5 shows the cumulative distribution function (CDF) of the obtained max-min secrecy rate of the multi-user MISO-OFDMA with the proposed optimization algorithm at a transmit power P_t of 30 dBm, a minimum required energy \tilde{E} of 10 mW and an energy harvesting efficiency \eta of 0.4. The max-min secrecy rate reaches 4.55 bps/Hz at a probability of 50\%. The minimum max-min secrecy rate is at 1.86 bps/Hz, and the maximum max-min secrecy rate is at 8.01 bps/Hz. A reasonably high max-min secrecy rate are obtained.

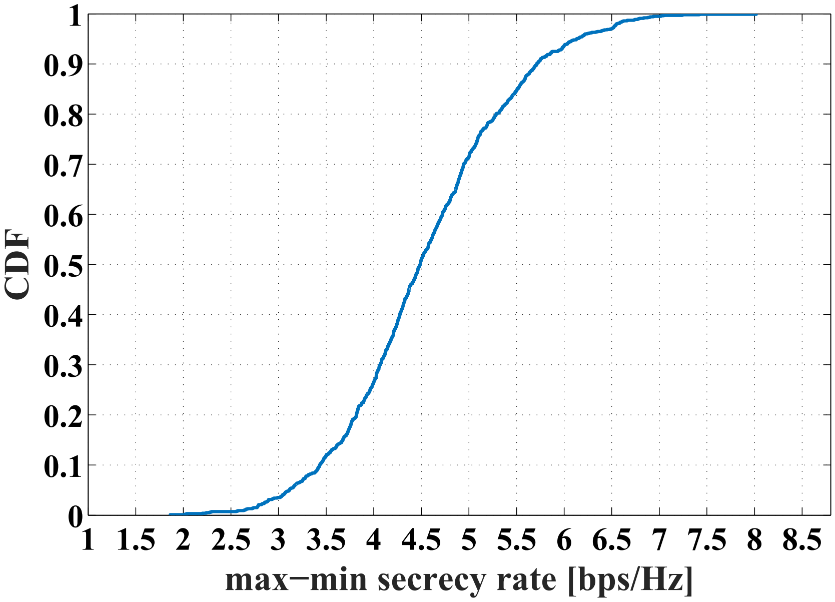


Fig. 5 CDF of the obtained max-min secrecy rate

Figure 6 illustrates an example of optimal subcarrier allocation at a realization of channel coefficients. It can be observed that all three users are equally allocated with two subcarriers. This result can be explained by using the max-min fairness criterion, where the optimal solution tends to make the secrecy rate of every user equal.

Figure 7 illustrates an example of optimal power splitting ratios at a realization of channel coefficients, where the power splitting ratios of the first, the second and the third users are 0.27287, 0.71688 and 0.61679 respectively. The highest power splitting ratio is assigned to the 2^{nd} user node, most likely to subdue its ability to eavesdrop other user nodes which might gain greater secrecy rate by decreasing R_{2,n}, n \in \{1,2,3,...,N\} in secrecy rate equation for any k \neq 2. On the other hand, the lowest power splitting ratio is assigned to the 1^{st} user node to increase its secrecy rate by boosting R_{1,n}, n \in \{1,2,3,...,N\} in secrecy rate equation when k=1.

Figure 8 shows the frequency of subcarrier allocation to each user node with 1,000 trials. Obviously, every subcarrier is allocated to all user nodes quite evenly due to the symmetry of the channel models of all user nodes. Specifically, the mean signal-to-noise ratios of all user nodes at each subcarrier are equal.

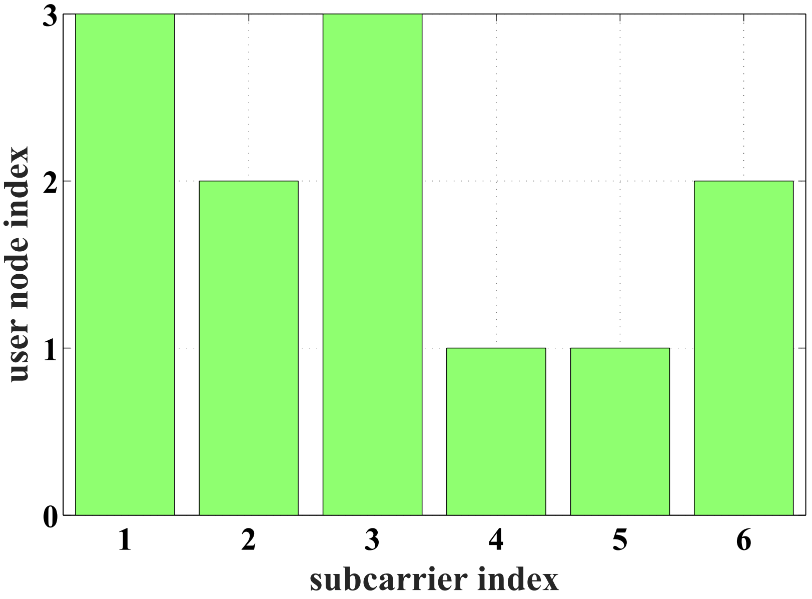


Fig. 6 An example of optimal subcarrier allocation

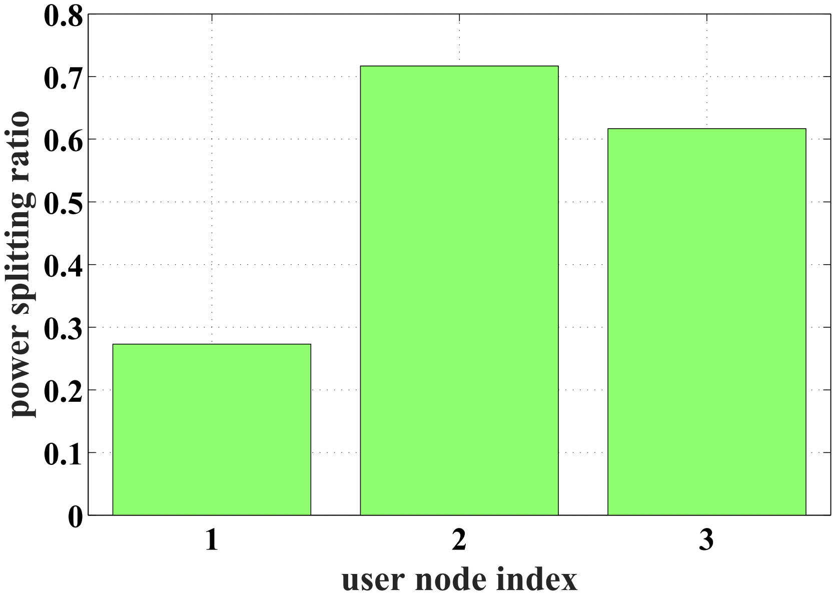


Fig. 7 An example of optimal power splitting ratios

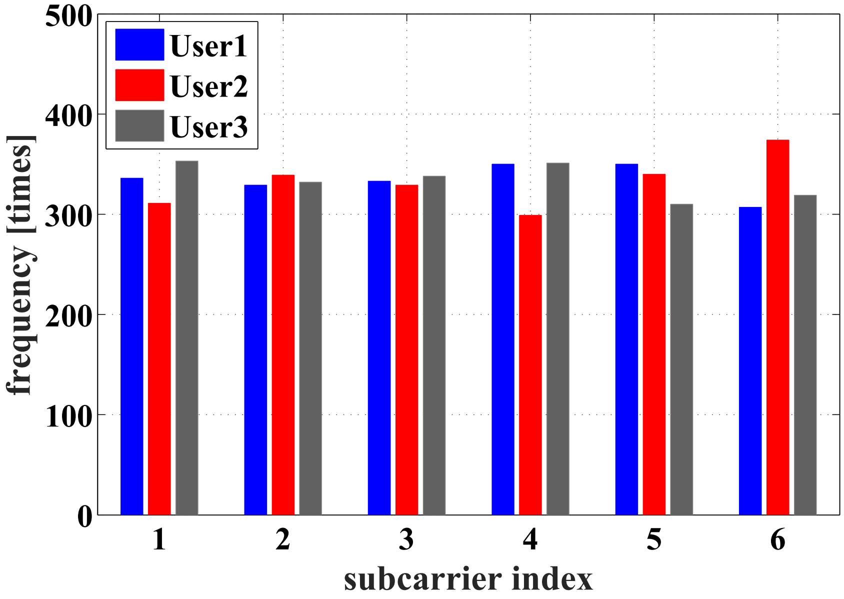


Fig. 8 Frequency of subcarrier allocation with 1,000 trials

Figure 9 shows the average max-min secrecy rate R^+ as a function of transmit power P_t at different minimum required harvested energy \tilde{E}, namely 10 mW, 30 mW, 50 mW and 100 mW. Due to the symmetry of all user nodes, only the max-min secrecy rate of the 1^{st} user node is used to calculate the average. The results are the same for all other user nodes. It can be observed that boosting the transmit power at the base station can raise the average max-min secrecy rate. Both the floor and ceiling exist when the transmit power becomes low and high, respectively. If the transmit power becomes too low, the average max-min secrecy rate will be zero. After boosting the transmit power beyond a level, the average max-min secrecy rate does not increase anymore. Hence, the simulation results give a design guideline to choose the transmit power high enough that the average max-min secrecy rate reaches the ceiling and not to raise the transmit power higher than that for energy efficiency. It can also be observed that the minimum required harvested energy affects both floor and ceiling by shifting the end of the floor regime and the beginning of the ceiling regime to higher transmit powers. A user node requires higher transmit power to achieve a non-zero average max-min secrecy rate at a greater minimum required harvested energy since a smaller fraction of energy is used for information demodulation and decoding. Also, a higher transmit power to reach the ceiling is required at greater minimum required harvested energy because less energy is available for information demodulation and decoding. Last, it can be seen that the different minimum required harvested energy values are associated with the same height of ceilings. This means that the minimum required harvested energy is irrelevant to the height of ceiling.

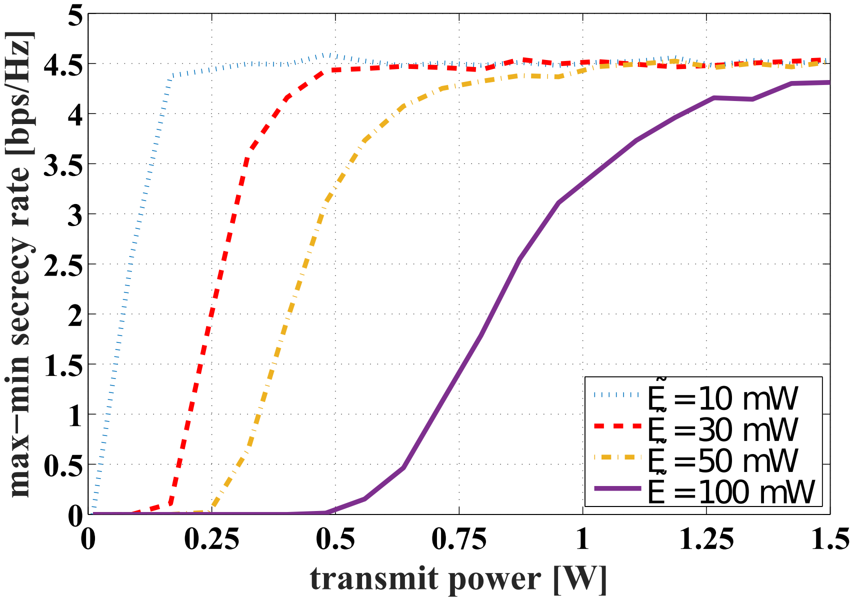


Fig. 9 Max-min secrecy rate as a function of transmit power P_t at different minimum energy requirement \tilde{E}

Figure 10 shows the average max-min secrecy rate R^+ as a function of the minimum required harvested energy \tilde{E} at different transmit power P_t, namely 0.5 W, 1 W and 1.5 W. When the transmit power is at 1.5 W, raising the minimum required harvested energy does not make the average max-min secrecy rate declines as long as the minimum required harvested energy is lower than 87 mW. In such regime, the performance is not limited by the minimum required harvested energy. When the minimum required harvested energy becomes higher than 87 mW, the average max-min secrecy rate declines until it reaches zero at a minimum required harvested energy of 320 mW or greater. The similar trends can be seen at a transmit power of 0.5 W and 1 W with the different end of the ceiling regime and the beginning of the floor regime, where a lower transmit power shifts them to the lower minimum required harvested energy due to the smaller power margin. In addition, a lower transmit power also makes the declining regime of the average max-min secrecy rate from the ceiling to the floor narrower.

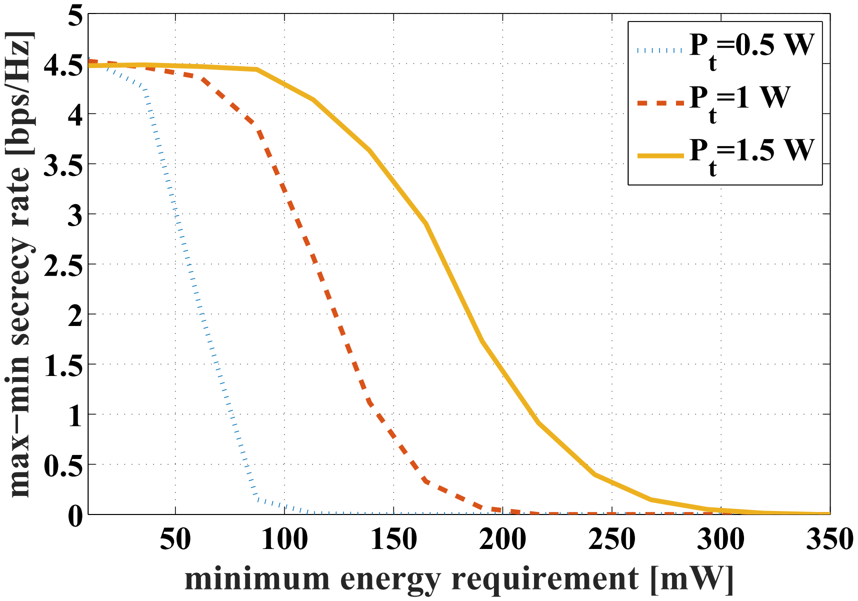


Fig. 10 Max-min secrecy rate as a function of minimum energy requirement \tilde{E} at different transmit power P_t

Figure 11 shows the average max-min secrecy rate R^+ as a function of energy harvesting efficiency \eta at different minimum required harvested energy \tilde{E}, namely 10 mW, 30 mW, 50 mW and 100 mW. The average max-min secrecy rate is obtained between the floor and the ceiling. When the energy harvesting efficiency is too low, a user node fails to harvest enough energy to meet the minimum required harvested energy, and the remaining signals for demodulation and decoding are too weak to achieve non-zero secrecy rate. At a higher minimum required harvested energy, the greater energy harvesting efficiency is necessary for obtaining non-zero average max-min secrecy rate. Changing minimum required harvested energy affects the end of the floor regime and the beginning of the ceiling regime, where a greater minimum required harvested energy shifts them to the higher energy harvesting energy. It can be seen that the different minimum required harvested energy values are associated with the same height of ceiling. This means that the minimum required harvested energy is irrelevant to the height of ceiling. Also, a smaller minimum required harvested energy makes the rising regime of the average max-min secrecy rate from the ceiling to the floor narrower.

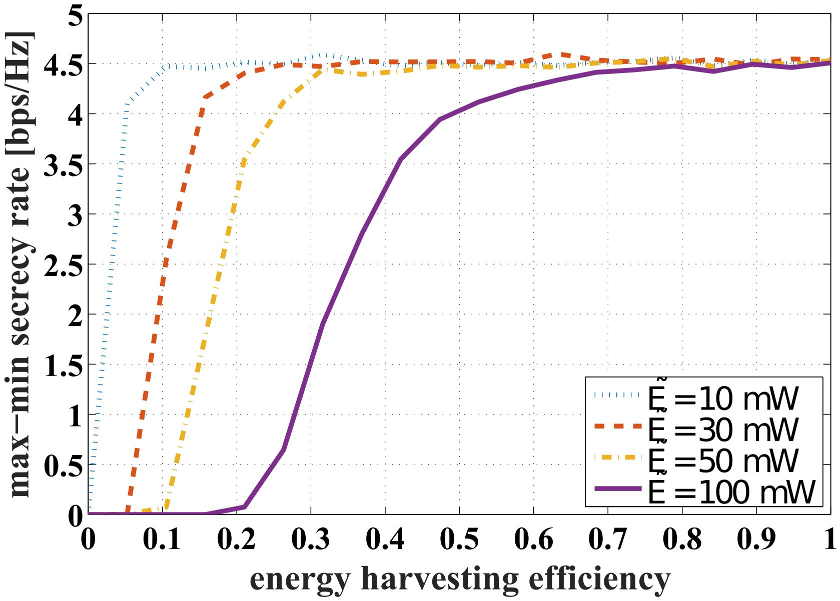


Fig. 11 Max-min secrecy rate as a function of energy harvesting efficiency \eta

Also, to illustrate the advantage of the proposed SF trellis codes over the conventional SF codes, we present the simulation results comparing OFDM symbol error rate in the frequency-selective Rayleigh fading channel. Each pair of transmit and receive antennas has 2 channel taps with uniform power delay profile. The time delay between 2 channel taps will be varied. The number of subcarriers is fixed at 128, and the cyclic prefix length is sufficient to cover the time delay. For fair comparison, all compared codes use 2 transmit antennas, 1 receive antenna, and provides a spectral efficiency of 1 bit/subcarrier.

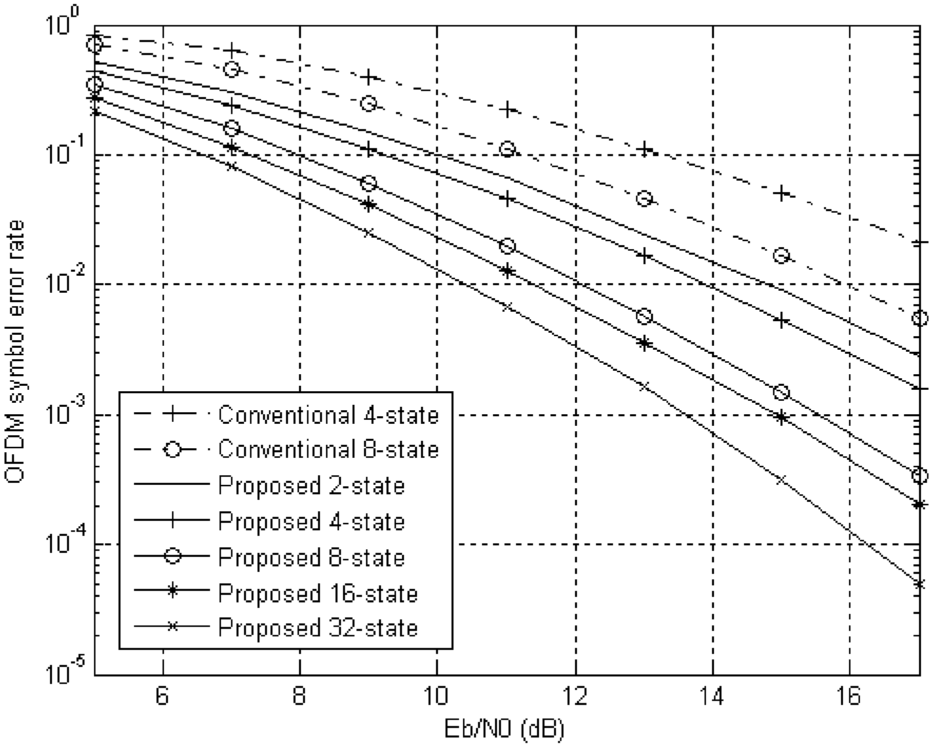


Fig. 12 SF codes comparison at a time delay of 5 samplings

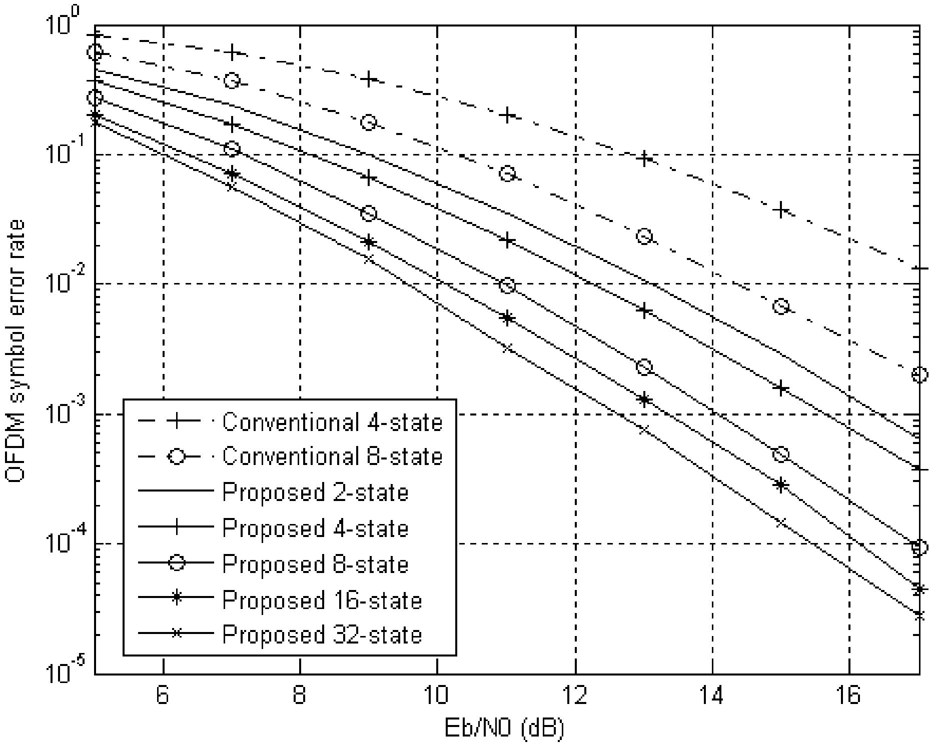


Fig. 13 SF codes comparison at a time delay of 10 samplings

Discussions

In Fig. 5, the max-min secrecy rate reaches 4.55 bps/Hz at a probability of 50%. The minimum max-min secrecy rate is at 1.86 bps/Hz, and the maximum max-min secrecy rate is at 8.01 bps/Hz. A reasonably high max-min secrecy rate are obtained.

In Fig. 6, all three users are equally allocated with two subcarriers. This result can be explained by using the max-min fairness criterion, where the optimal solution tends to make the secrecy rate of every user equal.

In Fig. 7, the highest power splitting ratio is assigned to the 2^{nd} user node, most likely to subdue its ability to eavesdrop other user nodes which might gain greater secrecy rate by decreasing R_{2,n}, n \in \{1,2,3,...,N\} for any k ≠ 2. On the other hand, the lowest power splitting ratio is assigned to the 1^{st} user node to increase its secrecy rate by boosting R_{1,n}, n \in \{1,2,3,...,N\} when k=1.

In Fig. 8, every subcarrier is allocated to all user nodes quite evenly due to the symmetry of the channel models of all user nodes. Specifically, the mean signal-to-noise ratios of all user nodes at each subcarrier are equal.

In Fig. 9, due to the symmetry of all user nodes, only the max-min secrecy rate of the 1^{st} user node is used to calculate the average. The results are the same for all other user nodes. It can be observed that boosting the transmit power at the base station can raise the average max-min secrecy rate. Both the floor and ceiling exist when the transmit power becomes low and high, respectively. If the transmit power becomes too low, the average max-min secrecy rate will be zero. After boosting the transmit power beyond a level, the average max-min secrecy rate does not increase anymore. Hence, the simulation results give a design guideline to choose the transmit power high enough that the average max-min secrecy rate reaches the ceiling and not to raise the transmit power higher than that for energy efficiency. It can also be observed that the minimum required harvested energy affects both floor and ceiling by shifting the end of the floor regime and the beginning of the ceiling regime to higher transmit powers. A user node requires higher transmit power to achieve a non-zero average max-min secrecy rate at a greater minimum required harvested energy since a smaller fraction of energy is used for information demodulation and decoding. Also, a higher transmit power to reach the ceiling is required at greater minimum required harvested energy because less energy is available for information demodulation and decoding. Last, it can be seen that the different minimum required harvested energy values are associated with the same height of ceilings. This means that the minimum required harvested energy is irrelevant to the height of ceiling.

In Fig. 10, when the transmit power is at 1.5 W, raising the minimum required harvested energy does not make the average max-min secrecy rate declines as long as the minimum required harvested energy is lower than 87 mW. In such regime, the performance is not limited by the minimum required harvested energy. When the minimum required harvested energy becomes higher than 87 mW, the average max-min secrecy rate declines until it reaches zero at a minimum required harvested energy of 320 mW or greater. The similar trends can be seen at a transmit power of 0.5 W and 1 W with the different end of the ceiling regime and the beginning of the floor regime, where a lower transmit power shifts them to the lower minimum required harvested energy due to the smaller power margin. In addition, a lower transmit power also makes the declining regime of the average max-min secrecy rate from the ceiling to the floor narrower.

In Fig. 11, the average max-min secrecy rate is obtained between the floor and the ceiling. When the energy harvesting efficiency is too low, a user node fails to harvest enough energy to meet the minimum required harvested energy, and the remaining signals for demodulation and decoding are too weak to achieve non-zero secrecy rate. At a higher minimum required harvested energy, the greater energy harvesting efficiency is necessary for obtaining non-zero average max-min secrecy rate. Changing minimum required harvested energy affects the end of the floor regime and the beginning of the ceiling regime, where a greater minimum required harvested energy shifts them to the higher energy harvesting energy. It can be seen that the different minimum required harvested energy values are associated with the same height of ceiling. This means that the minimum required harvested energy is irrelevant to the height of ceiling. Also, a smaller minimum required harvested energy makes the rising regime of the average max-min secrecy rate from the ceiling to the floor narrower.

In Fig. 12, we compare the proposed SF trellis code with the conventional SF trellis code, which also achieves both the frequency diversity and spatial diversity. The time delay between two taps is set at 5 samplings. The slopes of the curves verify that the proposed codes exploit full diversity. Moreover, the shifts to the left illustrate the significant coding gain from using the proposed method to design SF trellis codes instead of using the conventional method to obtain SF trellis codes via mapping.

In Fig. 13, we consider the similar comparison as in Fig. 12 except that the time delay between 2 channel taps is increased to 10 samplings. It can be observed that the slopes of all codes get steeper. This shows the effect of the varied time delay on the error rate of the full-diversity SF codes.

Conclusions

The proposed algorithm jointly optimizes the subcarrier allocation and power splitting ratio in the downlink multi-user SWIPT MISO-OFDMA to maximize the secrecy rate with max-min fairness, where all user nodes eavesdrop each other. The simulation results give a guideline for designing efficient network such as the appropriate transmit power at the base station. The floor and ceiling of average max-min secrecy rate exist, where the height of ceiling is not limited by the transmit power, the minimum required harvested energy, nor the energy harvesting efficiency. Even though the complexity of the proposed algorithm becomes high when the number of users and the number of subcarriers increase, it can serve as a performance benchmarking for other low complexity algorithm. Also, we have introduced a practical method to design space-frequency trellis codes for a system that combines space-time coding with OFDM. The designed SF codes obtain full spatial and frequency diversity, available in the frequency-selective channels. This is not achieved by the ST trellis codes that exploit only the spatial diversity. The proposed method is a good alternative to the conventional method, which constructs full-diversity SF trellis codes from ST trellis codes via mapping, because the better error rate performance can be obtained at the same spectral efficiency.

Future Directions

Since the proposed algorithm aims to get as close as possible to the optimal point, the computation complexity is high when the number of users or the number of subcarriers is high. The future direction is to find a sub-optimal algorithm where the complexity increases linearly or in the polynomial order with the number of users or the number of subcarriers, and the degradation of the performance is not significant.

Output จากโครงการวิจัยที่ได้รับทุนจาก สกว.

1. ผลงานตีพิมพ์ในวารสารวิชาการนานาชาติ (ระบุชื่อผู้แต่ง ชื่อเรื่อง ชื่อวารสาร ปี เล่มที่ เลขที่ และหน้า) หรือผลงานตามที่คาดไว้ในสัญญาโครงการ

    คาดว่าจะได้ผลงานตีพิมพ์ในวารสารวิชาการระดับนานาชาติที่อยู่ในฐานข้อมูล SCOPUS, Scientific Journal Ranking (SCIMAGO) อยู่ใน Q1 จำนวน 1 ฉบับ ขณะนี้อยู่ในขั้นตอนการจัดทำ reprint (Impact Factor 0.97) ดังภาคผนวก

2. การนำผลงานวิจัยไปใช้ประโยชน์
    - เชิงพาณิชย์ (มีการนำไปผลิต/ขาย/ก่อให้เกิดรายได้ หรือมีการนำไปประยุกต์ใช้โดยภาคธุรกิจ/บุคคลทั่วไป)

      ประยุกต์ใช้โดยภาคธุรกิจ โดยใช้ผลการวิจัยที่ได้เป็นข้อมูลประกอบการตัดสินใจทางเลือกทางเทคโนโลยีสำหรับเครือข่ายสื่อสารไร้สายในอนาคต
    - เชิงนโยบาย (มีการกำหนดนโยบายอิงงานวิจัย/เกิดมาตรการใหม่/เปลี่ยนแปลงระเบียบข้อบังคับหรือวิธีทำงาน)

      หน่วยงานที่ดูแลกำกับกิจการโทรคมนาคม เช่น กสทช. สามารถใช้ผลการวิจัยที่ได้เป็นข้อมูลประกอบการตัดสินใจวางนโยบายที่จะกำหนดทิศทางการใช้เทคโนโลยีสำหรับเครือข่ายไร้สายในอนาคต
    - เชิงสาธารณะ (มีเครือข่ายความร่วมมือ/สร้างกระแสความสนใจในวงกว้าง)

      เมื่อผลการวิจัยได้รับการเผยแพร่แล้ว นักวิจัยและนักพัฒนาสามารถศึกษาเพื่อให้เกิดแนวคิดต่อยอดการวิจัยพัฒนาเทคโนโลยีเครือข่ายสื่อสารไร้สายต่อไปได้
    - เชิงวิชาการ (มีการพัฒนาการเรียนการสอน/สร้างนักวิจัยใหม่)

      สร้างนักวิจัยใหม่ คือนายภูเบต แสงมะฮะหมัด ซึ่งเป็นนิสิตปริญญาโท โดยให้ช่วยเหลือปรับเปลี่ยนโปรแกรมจำลองด้วยคอมพิวเตอร์ และช่วยเก็บผลการจำลองด้วยคอมพิวเตอร์ ในระหว่างที่ให้ช่วยงานวิจัยนี้ ได้สอนให้นิสิตเข้าใจวิธีการที่ใช้ และอภิปรายผลการจำลองที่ได้ให้นิสิต หลังสำเร็จการศึกษา นิสิตได้ตำแหน่งอาจารย์มหาวิทยาลัย และได้ทุนศึกษาต่อระดับปริญญาเอก

3. อื่นๆ (เช่น ผลงานตีพิมพ์ในวารสารวิชาการในประเทศ การเสนอผลงานในที่ประชุมวิชาการ หนังสือ การจดสิทธิบัตร)

ภาคผนวก