Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving

Hao Li, Xianbin Wang, *Senior Member, IEEE*, and Jean-Yves Chouinard, *Senior Member, IEEE*

***Abstract*—In this paper, we present a novel eavesdropping-resilient OFDM system through sorted subcarrier interleaving. The transmitter interleaves subcarriers in each OFDM signal according to its dynamic channel state information (CSI) to the legitimate receiver. More specifically, subcarriers are interleaved according to the sorted order of their instantaneous channel gains that are observed at the transmitter. Based on channel reciprocity, the legitimate receiver can derive the interleaving pattern initiated by the transmitter through its local channel estimate, and then de-interleave the received signals. In contrast, since spatially separated wireless channels in rich multipath environments are independent of each other, an eavesdropper at a third location cannot follow the dynamic subcarrier interleaving permutation, and thus fails to eavesdrop this transmission. Considering the imperfect reciprocity of noisy channel estimates at the legitimate terminals, only a subset of subcarriers in each OFDM signal is involved in the interleaving. A subcarrier selection algorithm is investigated to realize a trade-off between the eavesdropping resilience and transmission reliability. Theoretical analysis and Monte Carlo simulations have been provided to validate the proposed system. Compared with prior security enhancement schemes, the proposed approach requires only minor modifications to off-the-shelf systems and avoids additional resource consumption.**

***Index Terms*—Security, wireless communications, OFDM, eavesdropping-resilient, subcarrier interleaving.**

I. Introduction

EAVESDROPPING is a critical security problem in wireless networks due to the inherent broadcast nature of wireless communications. Adversaries can possibly intercept the data traffic as long as they lie within the radio transmission coverage areas. Orthogonal frequency-division multiplexing (OFDM) has been widely adopted in modern wireless communication networks, because of its high spectral efficiency and robustness against multipath fading. Unfortunately, a conventional OFDM signal is vulnerable to eavesdropping attacks due to its distinct time and frequency characteristics, such as the time- and frequency-domain correlations and second-order cyclostationarity. Taking advantage of these characteristics, eavesdroppers can blindly estimate the transmission parameters of OFDM systems and then infer the transmitted information. Hence, it is of practical interest to enhance the built-in security of OFDM systems due to its wide popularity and inherent security weaknesses [1].

A. State of the Art in Eavesdropping Prevention

Traditional communications security mechanisms largely rely on cryptographic techniques at upper layers of the network protocol stacks, where the security is generally guaranteed by using either pre-distributed or public cryptography keys between communication nodes [2]. However, due to insufficient key updates and potential secrecy leakage in the key distribution, such highly standardized practices face severe threats of being cracked. Recently, new security paradigms that exploit the situation- and user-dependent randomness from wireless multipath channels to defend the transmission at the physical layer, are emerging as effective means to complement conventional wireless security techniques [1].

Several studies for preventing eavesdropping in wireless communication networks at the physical layer have been published. Information-theoretic security studies [3], [4] demonstrated the possibility of confidential communications under a Gaussian wiretap channel model when the legitimate receiver has a better channel condition, in terms of signal-to-noise ratio (SNR), than eavesdroppers. More recently, it was proved theoretically that in the presence of multipath fading, secure transmission is achievable even when eavesdroppers have higher average SNRs than the legitimate receiver [5], [6].

In addition to the demonstration of the feasibility to secure wireless communications at the physical layer, practical approaches that deal with eavesdropping at the physical layer have also been investigated. Artificial noise [7], [8] was generated using multiple antennas or cooperative nodes, and was injected into the null-subspace of the intended receiver's channel to prevent eavesdropping. In [9], transmitter beamforming was proposed to facilitate the transmission confidentiality, where the maximum secrecy sum rate was achieved when the eavesdropping channel was known. With the collaboration of user nodes in a cluster, an anti-eavesdropping space-time network coding scheme was proposed to prevent eavesdropping in [10]. Similarly, relay techniques were utilized to defend against eavesdroppers by increasing the secrecy rate at the cost of collaborative nodes [11], [12].

Several security approaches that are specially tailored for OFDM systems can also be found in the literature. Power and subcarrier allocation techniques were introduced to improve the security of OFDM systems against eavesdropping [13],

Manuscript received April 4, 2014; revised September 3, 2014; accepted October 16, 2014. Date of publication October 24, 2014; date of current version February 6, 2015. The associate editor coordinating the review of this paper and approving it for publication was G. Yue.

H. Li and X. Wang are with the Department of Electrical and Computer Engineering, Western University, London ON N6A 5B9, Canada (e-mail: hli347@uwo.ca; xianbin.wang@uwo.ca).

J.-Y. Chouinard is with the Department of Electrical and Computer Engineering, Laval University, Quebec City QC G1V 0A6, Canada (e-mail: jean-yves.chouinard@gel.ulaval.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2014.2365031

[14], with the information of eavesdropping channels. A secure OFDM system was reported in [15], where distributed transmitters independently sent pre-equalized OFDM signals to degrade eavesdropping channel conditions. In [16], the authors utilized chaos-based cryptography in combination with channel coding to enhance security, where secret keys were exchanged between legitimate parties. A constellation rotation technique was also proposed to prevent eavesdropping by using a pseudo random sequence generator shared in a network [17]. Moreover, a dynamic coordinate interleaving scheme was proposed in [18], under the condition that symbols to be transmitted in OFDM systems were modulated in a complex-signal form.

Both the general eavesdropping defense methods and specially designed OFDM security schemes are able to enhance the transmission security of OFDM systems at the physical layer. However, the aforementioned security approaches require either additional resources such as information of eavesdropping channel, cooperating nodes and multiple antennas, or significant changes of existing network protocols and device hardware. In addition, most of them have high computational complexity. Effective alternatives with minimum resource requirements, minor modifications to off-the-shelf systems and low operational complexity have yet to be investigated.

B. Contributions of the Proposed Secure OFDM System

An effective and simple eavesdropping-resilient OFDM system is proposed in this paper. Relying on the dynamic channel state information (CSI) between legitimate users, a subset of subcarriers in each OFDM signal is selected and then interleaved according to the decreasing order of their channel gains. Based on channel reciprocity, the CSI-based subcarrier interleaving permutation can be shared between legitimate terminals without any signaling. Due to the independence between spatially separated wireless channels, legitimate and eavesdropping channels are uncorrelated. It is thus hard for eavesdroppers to deduce the dynamic interleaving pattern and then to recover the transmitted information. The main advantages of the proposed security approach, i.e., CSI-based sorted subcarrier interleaving, and contributions of the paper itself, are summarized as follows:

- We investigate CSI-based sorted subcarrier interleaving to overcome passive eavesdropping. Although subcarrier interleaving has been introduced into OFDM systems to improve the transmission reliability [19]–[21], to the best knowledge of the authors, it is the first work to employ subcarrier interleaving to enhance the transmission security. Compared with prior works, the proposed scheme guarantees computational security with only minor modifications of existing systems. In addition, it avoids additional resource consumption and involves limited computational complexity.
- The impact of imperfect reciprocity of channel estimates at the legitimate communicating pair, which is induced by noisy channel estimations, is addressed in the design. A subcarrier selection algorithm is investigated to achieve a trade-off between the resilience against eavesdropping and reliability of legitimate transmission.

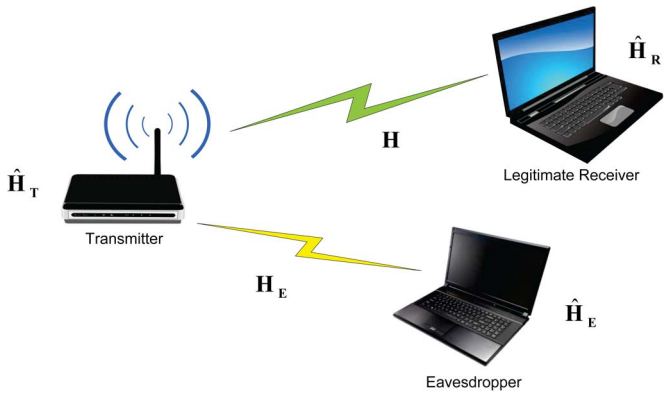

Fig. 1. A wireless communication scenario consisting of two legitimate terminals and an eavesdropper.

- The symbol error rate (SER) of eavesdropping, information leakage at the eavesdropper and security against brute force attacks are analyzed to prove the security of the proposed approach. SER of legitimate transmission is derived to evaluate the transmission reliability of the proposed system. Monte Carlo simulation results have been provided to validate this design. Compared with the conventional OFDM system, our approach is much more resilient to eavesdropping and at almost no cost of transmission reliability.

Organization: The remainder of this paper is organized as follows. Section II introduces the system model and relevant background about multipath channel estimates in OFDM systems. The proposed eavesdropping-resilient OFDM system is described in Section III, followed by a performance evaluation in Section IV. The interleaved subcarrier selection algorithm is investigated in Section V. Simulation results to validate the proposed system are provided in Section VI. Finally, conclusions are drawn in Section VII.

Notation: Throughout the paper, bold letters identify vectors and matrices, e.g., $\mathbf{H}_T$. Complex Gaussian random variable X with mean μ, variance σ^2, and with independent and identically distributed (i.i.d.) real and imaginary components is denoted as: $X \sim CN(\mu, \sigma^2)$.

II. Problem Formulation and Preliminaries

A. System Model

The wireless communication system model considered in this paper is depicted in Fig. 1. A source node communicates with a legitimate receiver in a richly scattered radio environment, in the presence of a passive and silent eavesdropper. OFDM is adopted for the transmission between legitimate users, and the eavesdropper also has the capability to demodulate OFDM signals. Moreover, the eavesdropper can intercept all transmissions between legitimate users, but is not interested in disrupting the legitimate transmission. The forward and reverse channels between legitimate users occupy the same frequency band. A slow fading channel condition is considered, so that the forward and reverse channels remain constant over several time slots. In addition, the underlying noise and interference in both the main channel (between the transmitter

and intended receiver) and eavesdropping channel (between the transmitter and eavesdropper) are modeled as additive white Gaussian noise (AWGN).

Generally, a third party, who is at a distance larger than half a wavelength from the intended receiver, experiences fading conditions that are uncorrelated to those between the original legitimate communicating terminals [22]. For instance, in the 2.4 GHz frequency band, an eavesdropper which is roughly 6.25 cm away from the legitimate receiver would be affected by an eavesdropping channel independent of the main channel. In most practical scenarios, the eavesdropper has to be sufficiently separated from the legitimate terminals to avoid being detected, that is, with a distance of more than half a wavelength. Therefore, the distance between the legitimate receiver and eavesdropper is assumed to be larger than half a wavelength in this paper. The main channel and eavesdropping channel are thus modeled as independent channels.

B. Multipath Channel in OFDM Systems

Consider an OFDM system with N subcarriers. The discrete-frequency channel transfer function at the kth subcarrier, $H(k)$, can be given by

$$H(k)=\frac{1}{\sqrt{N}}\sum_{n=0}^{L-1}h(n)e^{-j2\pi\frac{kn}{N}},\quad k=0,1,\ldots,N-1, \quad (1)$$

where $h(n)$ denotes the channel impulse response's coefficient associated with the nth discrete-time channel tap. In a Rayleigh fading channel, for $n=0,1,\ldots,L-1$, the $h(n)$ coefficients can be modeled as i.i.d. zero-mean complex Gaussian random variables. As a linear combination of L Gaussian variables, $H(k), k=0,1,\ldots,N-1$ follows a distribution $CN(0,\sigma_H^2)$. The N subcarrier channels are identically distributed but may not be independent of each other. To simplify the mathematical analysis, we assume that all subcarriers experience i.i.d. fading. Consequently, the N subcarriers of each OFDM signal can be treated independently.

C. Principles Behind the Proposed Design

The randomness of wireless multipath channels is exploited to enhance the transmission security at the physical layer in the proposed OFDM system, by taking advantage of its reciprocity, spatial decorrelation and time variation characteristics.

Channel reciprocity indicates that a wireless channel behaves in an identical manner irrespective of in which direction it is observed. Theoretically, the transmitter and legitimate receiver would have an identical estimate of the main channel $H(k)$. In practice however, all the nodes in a network can only obtain noisy versions of the channels, because of estimation errors at channel estimators that are induced by interference, noise, as well as hardware limitations [23]. Thus, the frequency domain channel responses observed at the legitimate nodes during a channel coherence time take the form:

$$\hat{H}_T(k)=H(k)+\Delta H_T(k),\quad k=0,1,\ldots,N-1, \quad (2)$$

and

$$\hat{H}_R(k)=H(k)+\Delta H_R(k),\quad k=0,1,\ldots,N-1, \quad (3)$$

where $\hat{H}_T(k)$ and $\hat{H}_R(k)$ denote the estimates of $H(k)$ at the transmitter and legitimate receiver, respectively. $\Delta H_T(k)$ and $\Delta H_R(k)$ are the corresponding estimation errors, which can be modeled as zero-mean Gaussian random variables. Since the two terminals of a communication link generally experience independent interference and noise, $\Delta H_T(k)$ and $\Delta H_R(k)$ can be considered as statistically independent. Moreover, following the assumption that $H(k)$ of all N subcarriers are i.i.d., $\Delta H_{T/R}(k)$ for $k=0,1,\ldots,N-1$ should also be statistically independent but may not be identically distributed. To facilitate the analysis, we assume that $\Delta H_{T/R}(k)$ for all N subcarriers are i.i.d. in the following discussion, so that

$$\Delta H_{T/R}(k)\sim CN\left(0,\sigma_{T/R}^2\right). \quad (4)$$

Consequently, the estimates of the main channel at the transmitter and intended receiver are correlated, but may not be perfectly reciprocal.

Channel spatial decorrelation means that wireless channels associated with different endpoints at separate locations typically exhibit uncorrelated propagation characteristics. As a result, for an eavesdropper at a third location, the eavesdropping channel $H_E(k)$ would be uncorrelated with the main channel $H(k)$. The noisy channel observations at the eavesdropper, $\hat{H}_E(k)$, can be written as

$$\hat{H}_E(k)=H_E(k)+\Delta H_E(k),\quad k=0,1,\ldots,N-1. \quad (5)$$

Similarly, the channel estimation error $\Delta H_E(k)$ follows a complex Gaussian distribution $CN(0,\sigma_E^2)$ and $\hat{H}_E(k)$ of all N subcarriers can be modeled as i.i.d. complex Gaussian variables. Since $\Delta H_E(k)$ is also independent of $\Delta H_T(k)$ and $\Delta H_R(k)$, $\hat{H}_E(k)$ should be independent of the estimates $\hat{H}_T(k)$ and $\hat{H}_R(k)$ obtained at legitimate terminals.

Time variation means that wireless channels are time-varying and are able to introduce frequently updated randomness. The CSI-based security design would thus be updated frequently, which further strengthens its security.

III. Proposed Secure OFDM System With Sorted Subcarrier Interleaving

The proposed eavesdropping-resilient OFDM system with sorted subcarrier interleaving is illustrated in Fig. 2. At the transmitter end, M out of the N subcarriers of each OFDM signal are selected and interleaved after the symbol modulation. Accordingly, subcarrier deinterleaving is carried out between the equalization and symbol demodulation processes at the receiver end. The selection of the M interleaved subcarriers and their interleaving permutation are determined by the real-time CSI between the transmitter and legitimate receiver. The other processing steps of the proposed system are identical to those of a conventional OFDM system. It is noteworthy that the transmitter and legitimate receiver would estimate the main channel and determine the subcarrier interleaving pattern individually based on channel reciprocity. No sharing of their CSI estimates is required and allowed.

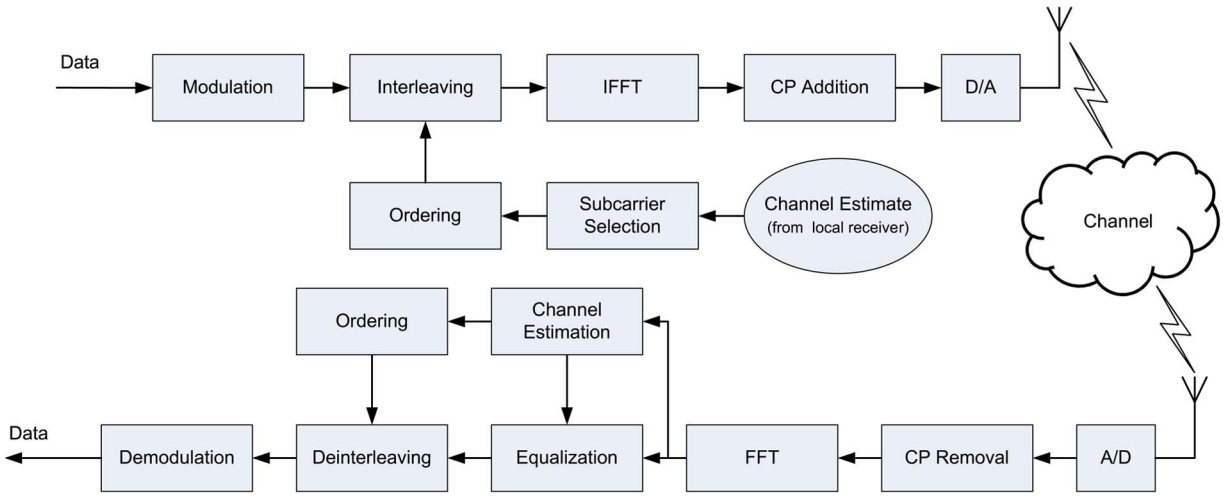

Fig. 2. Block diagram of the proposed eavesdropping-resilient OFDM system.

A. Selection of Interleaved Subcarriers

Due to the presence of channel estimation errors, channel observations at the transmitter and legitimate receiver are not perfectly reciprocal. To mitigate the impairment caused by imperfect reciprocity, only a subset of $M \leq N$ subcarriers in each OFDM signal, which can provide an interleaving pattern robust against imperfectly reciprocal channel estimates under an instantaneous channel condition, is selected for the dynamic interleaving at the transmitter. A trade-off between the resilience to eavesdropping and reliability of legitimate transmission is realized with a proposed subcarrier selection algorithm. A detailed discussion of this subcarrier selection algorithm will be presented in Section V, after analyzing how the proposed interleaving scheme acts on the performances of eavesdropping prevention and legitimate transmission in Section IV. Let $\mathcal{M}$ denote the subset of subcarriers involved in the dynamic subcarrier interleaving. The selection result ξ can be expressed as

$$\xi(k) = \begin{cases} 1, & k \in \mathcal{M} \\ 0, & k \notin \mathcal{M} \end{cases}, \quad k = 0, 1, \ldots, N-1. \tag{6}$$

Due to the channel reciprocity, the legitimate receiver is able to determine ξ based on its own channel estimate $\hat{\mathbf{H}}_R$. However, a mismatched ξ may occur due to an asymmetric CSI observation, particularly in an extremely hostile communication environment. This would cause several transmission errors. As will be shown in Section IV, the eavesdropping prevention capability of the proposed system is dominated by the subcarrier interleaving permutation, rather than the side information ξ. Thus, ξ can alternatively be sent out by the transmitter to improve the reliability of legitimate transmission, though this operation faces a potential threat of leakage of the information ξ. Whether or not to share the subcarrier selection result ξ would depend on the transmission reliability requirements and channel conditions. In the presented system design, ξ is transmitted from the transmitter to the legitimate receiver along with the data traffic, to achieve a low error rate transmission. It must be emphasized that it is not necessary to share this side information.

B. Subcarrier Interleaving

After the subcarrier selection, the M collected subcarriers are interleaved according to the descending order of their channel gains observed at the transmitter. The order of the M subcarriers can be expressed as

$$\left|\hat{H}_T(0)_k\right|^2 \geq \cdots \geq \left|\hat{H}_T(\iota)_k\right|^2 \geq \cdots \geq \left|\hat{H}_T(M-1)_k\right|^2. \tag{7}$$

Indices k and ι are included in the subcarrier specification. k denotes the exact position of the subcarrier among the N subcarriers and ι indicates the subcarrier order, among the M selected subcarriers, sorted according to the channel gains. It is noteworthy that the proposed scheme does not change the subcarrier allocation and utilization of all N subcarriers in each OFDM signal. Similar to the traditional interleaving in a conventional OFDM system, the only modification is the actual order of the M collected subcarriers. As this operation may also spread the errors out in the bit stream, the proposed sorted subcarrier interleaving is able to improve the transmission performance in addition to its security achievement.

The dynamic interleaving permutation of the M collected subcarriers is kept privately at the transmitter. The legitimate receiver would derive the interleaving permutation from its local estimate of the main channel based on channel reciprocity, and then de-interleave the received signal. To intercept the transmitted information, the eavesdropper has to locally determine the interleaving pattern, either by random guesses or brute force attacks, as there is no way for it to obtain the CSI of the main channel as well as the interleaving pattern initiated at the transmitter.

IV. Performance Evaluation

A. Security of the Proposed OFDM System

The security of the proposed OFDM system is evaluated through the SER of the eavesdropper that randomly guesses the interleaving pattern, the information leakage at the eavesdropper, as well as the robustness of the design against brute force attacks.

1) SER of Eavesdropping: As discussed in Section II-C, the channel observations $\hat{\mathbf{H}}_E$ are independent of $\hat{\mathbf{H}}_T$, so that the channel-gain orders obtained by the eavesdropper and transmitter are also statistically independent. Consequently, the eavesdropper has no more information than a random guess about the interleaving pattern. An interleaving permutation developed from an uncorrelated channel can also be considered as a random guess of the interleaving pattern initiated at the transmitter.

Considering that the eavesdropper can possibly intercept the subcerrier selection result ξ which is transmitted along with the data traffic, two scenarios are taken into consideration in the SER evaluation: the eavesdropper with or without the knowledge of ξ. If the subcarrier selection result ξ is known, the eavesdropper only needs to guess the subcarrier interleaving permutation. Because there are $M!$ possible permutations from the M selected subcarriers, and assuming that they are equiprobable, the probability that the eavesdropper derives an interleaving permutation identical to that developed by the transmitter, P_{E_M}, is

$$P_{E_M} = \frac{1}{M!}. \tag{8}$$

For the case where the eavesdropper has no information about ξ, it has to guess the actual selection of the M interleaved subcarriers in each OFDM signal, in addition to guessing the interleaving permutation. As a result, the probability that the eavesdropper derives the correct interleaving pattern without the side information ξ, $P_{E_{NM}}$, is

$$\begin{aligned} P_{E_{NM}} &= \frac{1}{\binom{N}{M}} \frac{1}{M!} \\ &= \frac{(N-M)!}{N!}. \end{aligned} \tag{9}$$

Clearly, $P_{E_{NM}}$ is smaller than P_{E_M} when $M \neq N$. However, P_{E_M} can already be quite low even if M is small. For instance, when $M = 8$, P_{E_M} can be as low as 2.5×10^{-5}. Therefore, the interception of the side information ξ at the eavesdropper will not severely affect the eavesdropping prevention capability of the proposed system, owing to the security achievement obtained from the interleaving permutation. Even if the eavesdropper has by "chance" obtained the subcarrier selection ξ, eavesdropping is still difficult. As a result, the subcarrier selection result ξ can be sent out by the transmitter to improve the reliability of legitimate transmissions.

Let P_S denote the SER of a conventional OFDM system using a given modulation scheme in a multipath fading channel. The SER of eavesdropping under the same channel condition when legitimate users adopt the proposed eavesdropping-resilient OFDM system, $P_{S,E}$, can be evaluated as

$$P_{S,E} = \begin{cases} 1 - P_{E_M}(1 - P_S), & \text{with } \xi \\ 1 - P_{E_{NM}}(1 - P_S), & \text{without } \xi. \end{cases} \tag{10}$$

2) Information Leakage at the Eavesdropper: Let us consider the worse case that the selection of interleaved subcarriers has been intercepted by the eavesdropper. At the eavesdropper's end, the bit error rate for each OFDM subcarrier in the proposed system can be approximated as

$$p_k \approx \begin{cases} \frac{1}{M!}\frac{P_o}{\alpha} + \left(1 - \frac{1}{M!}\right)\frac{1}{2}, & k \in \mathcal{M} \\ \frac{P_o}{\alpha}, & k \notin \mathcal{M}, \end{cases} \tag{11}$$

where P_o denotes the SER of a modulation scheme at a subcarrier, and α denotes the number of bits per symbol at that subcarrier. Assuming that each transmitted bit has an equal probability of being 0 and 1, the mutual information between the transmitted data X and data recovered at the eavesdropper, Y_E, can be derived as

$$\begin{aligned} I_k(Y_E; X) &= \mathbb{H}_k(Y_E) - \mathbb{H}_k(Y_E|X) \\ &= 1 + p_k \log_2 p_k + (1 - p_k)\log_2(1 - p_k), \end{aligned} \tag{12}$$

where $\mathbb{H}(\cdot)$ denotes the entropy operation.

With respect to the whole OFDM signal with N subcarriers, its information leakage can be calculated as

$$L_{OFDM} = \sum_{k=0}^{N-1} I_k(Y_E; X). \tag{13}$$

Therefore, the information leakage at the eavesdropper in the proposed eavesdropping-resilient OFDM system would be

$$\begin{aligned} &L_{OFDM} \\ &= M\left\{\left[\frac{P_o}{\alpha M!} + \left(\frac{1}{2} - \frac{1}{2M!}\right)\right]\log_2\left[\frac{P_o}{\alpha M!} + \left(\frac{1}{2} - \frac{1}{2M!}\right)\right]\right. \\ &\quad \left. + \left[\left(\frac{1}{2} + \frac{1}{2M!}\right) - \frac{P_o}{\alpha M!}\right]\log_2\left[\left(\frac{1}{2} + \frac{1}{2M!}\right) - \frac{P_o}{\alpha M!}\right]\right\} \\ &\quad + (N - M)\left[\frac{P_o}{\alpha}\log_2\frac{P_o}{\alpha} + \left(1 - \frac{P_o}{\alpha}\right)\log_2\left(1 - \frac{P_o}{\alpha}\right)\right] \\ &\quad + N. \end{aligned} \tag{14}$$

3) Security Against Brute Force Attacks: Under brute force attacks, it is true that the eavesdropper with unlimited power and storage can perform an exhaustive search and test all $M!$ permutations of each interleaving pattern and then retrieve the original signal. However, the proposed scheme can benefit from the continued influx of channel randomness and thus defend against brute force attacks. Along with the inherent variations of the wireless channel, the subcarrier interleaving pattern adopted by the transmitter is updated each channel coherence time. Meanwhile, the interleaving patterns are independent from one to another. Consequently, as long as the eavesdropper cannot break an interleaving pattern within a channel coherence time period, the time needed to retrieve the transmitted data would be accumulated as legitimate transmission goes on. This renders exhaustive brute force attacks impractical after several sequential transmissions.

In most practical scenarios, the channel coherence time is much shorter than the time cost of each brute force attack. Consider for instance a WiFi system. In a 2.4 GHz WiFi channel, which is usually considered as a slow time-varying wireless channel, the channel coherence time is approximately 53 ms for a typical pedestrian walking speed of 1 m/s. On the

other hand, it has been demonstrated that a brute force attack would take at least 4 hours to crack an 8-digit pin in WiFi systems that requires $11000/2 = 5500$ attempts on average [24]. In other words, each attempt of the brute force attack would take at least $(4 \times 3600)/5500 = 2.62$ s. As a result, packets with $2620/53 = 49$ independent interleaving patterns will be transmitted within the duration of each attempt of the brute force attack. For the case that only 8 subcarriers are involved in the sorted interleaving in the proposed system, where a brute force attack on each interleaving pattern would require $8!/2 = 20160$ attempts on average, the interception for a 10 minutes worth of legitimate transmission would take $(10 \times 60/0.053) \times 20160 \times 2.62 \approx 166100$ hours. Brute force attacks are even more impractical when more subcarriers are included in the CSI-based subcarrier interleaving, when the subcarrier interleaving pattern is updated more frequenctly under faster channel variations, and when the legitimate transmission lasts longer.

B. Reliability of Legitimate Transmission

The reliability of legitimate transmission is evaluated in terms of SER at the legitimate receiver. Since the instantaneous subcarrier selection result ξ is sent to the intended receiver by the transmitter, errors caused by inaccurate estimations of ξ at the legitimate receiver are ignored in the following analysis.

Substituting (2) into (3), the channel estimate at the legitimate receiver can be rewritten as

$$\begin{aligned}\hat{H}_R(k) &= \hat{H}_T(k) - \Delta H_T(k) + \Delta H_R(k) \\ &= \hat{H}_T(k) + \Delta H_{TR}(k), \quad k = 0, 1, \ldots, N-1, \end{aligned} \tag{15}$$

where $\Delta H_{TR}(k) = -\Delta H_T(k) + \Delta H_R(k)$. As shown in (15), the estimate $\hat{H}_R(k)$ that is observed by the legitimate receiver can be considered as a noisy version of $\hat{H}_T(k)$ that has been previously obtained and used to determine the interleaving pattern at the transmitter. Given a channel response $\hat{H}_T(k)$, $\hat{H}_R(k)$ can be modeled as a complex Gaussian random variable with mean $\hat{H}_T(k)$ and variance $\sigma_{TR}^2 = \sigma_T^2 + \sigma_R^2$. The channel gain $\hat{\lambda}_{Rk} = |\hat{H}_R(k)|^2$ thus follows a noncentral chi-square distribution with 2 degrees of freedom, with a probability density function (PDF)

$$f_{Rk}(\hat{\lambda}_{Rk}) = \frac{1}{\sigma_{TR}^2} e^{-\left(\frac{|\hat{H}_T(k)|^2 + \hat{\lambda}_{Rk}}{\sigma_{TR}^2}\right)} I_0\left(\frac{\sqrt{\hat{\lambda}_{Rk}\left|\hat{H}_T(k)\right|^2}}{2\sigma_{TR}^2}\right), \tag{16}$$

where $I_\theta(x)$ represents the θth order modified Bessel function of the first kind:

$$I_\theta(x) = \sum_{k=0}^{\infty} \frac{(x/2)^{\theta+2k}}{k!\Gamma(\theta + k + 1)}. \tag{17}$$

It is noteworthy that the PDFs $f_{Rk}(\hat{\lambda}_{Rk})$ for different subcarriers are not identical since they may have different noncentralized parameters $|\hat{H}_T(k)|^2$.

Let Φ_T denote the event that $|\hat{H}_T(0)_k|^2 \geq \cdots \geq |\hat{H}_T(\iota)_k|^2 \geq \cdots \geq |\hat{H}_T(M-1)_k|^2$ and Φ_R denote the event that $|\hat{H}_R(0)_k|^2 \geq \cdots \geq |\hat{H}_R(\iota)_k|^2 \geq \cdots \geq |\hat{H}_R(M-1)_k|^2$. The probability, P_L, that the legitimate receiver derives the correct interleaving permutation from its channel estimate $\hat{\mathbf{H}}_\mathbf{R}$ is then

$$\begin{aligned} P_L &= \sum^{M!} \frac{1}{M!} P(\Phi_R|\Phi_T) \\ &= \frac{P(\Phi_R \cap \Phi_T)}{P(\Phi_T)}. \end{aligned} \tag{18}$$

For M independent subcarriers, each potential order happens with equal probability $P(\Phi_T) = 1/M!$. Referring to the order statistics theory [25], $P(\Phi_R \cap \Phi_T)$ can be calculated as

$$\begin{aligned} &P(\Phi_R \cap \Phi_T) \\ &= \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{T0}}^{+\infty} \cdots \int_{\hat{\lambda}_{T(M-2)}}^{+\infty} f\left(\hat{\lambda}_{T0}, \ldots, \hat{\lambda}_{T(M-1)}\right) \\ &\quad \left\{ \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{R0}}^{+\infty} \cdots \int_{\hat{\lambda}_{R(M-2)}}^{+\infty} f\left(\hat{\lambda}_{R0}, \ldots, \hat{\lambda}_{R(M-1)}\right) \right. \\ &\quad \left. \times d\hat{\lambda}_{R0}\, d\hat{\lambda}_{R1} \cdots d\hat{\lambda}_{R(M-1)} \right\} d\hat{\lambda}_{T0}\, d\hat{\lambda}_{T1} \cdots d\hat{\lambda}_{T(M-1)}, \end{aligned} \tag{19}$$

where $f(\hat{\lambda}_{R0}, \ldots, \hat{\lambda}_{R(M-1)})$ denotes the joint PDF of the M subcarrier channel gains observed at the legitimate receiver. Because the subcarrier channel gains are independent of each other, this joint PDF can be rewritten as

$$f\left(\hat{\lambda}_{R0}, \ldots, \hat{\lambda}_{R(M-1)}\right) = \prod_{\iota=0}^{M-1} f_{R\iota}(\hat{\lambda}_{R\iota}). \tag{20}$$

Substituting (20) into (19), we have

$$\begin{aligned} &P(\Phi_R \cap \Phi_T) \\ &= \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{T0}}^{+\infty} \cdots \int_{\hat{\lambda}_{T(M-2)}}^{+\infty} f\left(\hat{\lambda}_{T0}\right) \cdots f\left(\hat{\lambda}_{T(M-1)}\right) \\ &\quad \left\{ \int_{-\infty}^{+\infty} f_{R0}(\hat{\lambda}_{R0})\, d\hat{\lambda}_{R0} \int_{\hat{\lambda}_{R0}}^{+\infty} f_{R1}(\hat{\lambda}_{R1})\, d\hat{\lambda}_{R1} \cdots \right. \\ &\quad \left. \cdots \int_{\hat{\lambda}_{R(M-2)}}^{+\infty} f_{R(M-1)}(\hat{\lambda}_{R(M-1)})\, d\hat{\lambda}_{R(M-1)} \right\} \\ &\quad \times d\hat{\lambda}_{T0}\, d\hat{\lambda}_{T1} \cdots d\hat{\lambda}_{T(M-1)}. \end{aligned} \tag{21}$$

Since (21) involves integration with Bessel functions, it cannot be worked out analytically. As a result, the probability of deriving an identical interleaving permutation at the legitimate user, P_L, cannot be expressed in a closed form. Computer simulations were carried out to evaluate this probability P_L: these are presented in Section VI. As the SER analysis for the eavesdropper's end, the SER at the legitimate receiver of the proposed OFDM system can be given by

$$P_{S,L} = 1 - P_L(1 - P_S). \tag{22}$$

V. Interleaved Subcarrier Selection Algorithm

It can be concluded from the performance evaluation that the selection of the interleaved subcarrier subset $\mathcal{M}$ impacts both the eavesdropping resilience and transmission reliability of the proposed OFDM system. Its security is determined by the subset size M while the transmission reliability depends on both M and channel gains of subcarriers involved in the interleaving process, i.e., $|\hat{H}_T(k)|^2$ for $k \in \mathcal{M}$. To collect a subcarrier subset $\mathcal{M}$ that can make the interleaving pattern unrecognizable to the eavesdropper while being robust against imperfectly reciprocal channel estimates between the legitimate participants, two questions need to be answered: 1) How many subcarriers have to be interleaved? 2) Which M out of the N subcarriers should be selected?

A. Size M of the Interleaved Subcarrier Subset $\mathcal{M}$

As shown in (8) and (9), the probability that an eavesdropper successfully derives the interleaving permutation used by the transmitter is uniquely determined by the size, M, of the set of interleaved subcarriers. Since a system that can successfully defend itself against eavesdropping with the side information ξ should also perform well when ξ is not available to the eavesdropper, the minimum number of interleaved subcarriers, M_{min}, can be determined from P_{E_M}. Given the constraint of P_{E_M} in preventing eavesdropping, Ω, M_{min} can be derived by finding the inverse factorial of $1/\Omega$, that is

$$M_{min} = \left\lceil F_{IF}\left(\frac{1}{\Omega}\right)\right\rceil, \tag{23}$$

where $F_{IF}(\cdot)$ denotes the inverse factorial function and $\lceil\cdot\rceil$ is the ceiling function.

B. Selection of the M Interleaved Subcarriers

Once the minimum size of the interleaved subcarrier subset is determined, M out of the N subcarriers in an OFDM signal that provide a subcarrier interleaving permutation robust to imperfectly reciprocal channel observations between legitimate communicating pair can be selected. Since the selected subcarriers are to be interleaved according to the sorted order of their channel gains, an interleaving permutation should be more insensitive to channel estimation errors if any two adjacent interleaved subcarriers have a larger channel gain difference.

Given two subcarriers, i and j, with channel gains $|\hat{H}_T(i)|^2 \geq |\hat{H}_T(j)|^2$ at the transmitter, the order mismatch probability of these two subcarriers at the legitimate receiver, P_e, can be given by

$$\begin{aligned} P_e &= P\left\{\left|\hat{H}_R(i)\right|^2 < \left|\hat{H}_R(j)\right|^2\right\} \\ &= P\left\{\left|\hat{H}_R(i)\right|^2 - \left|\hat{H}_R(j)\right|^2 < 0\right\}. \end{aligned} \tag{24}$$

Based on the statistical theory result about the difference of two independent noncentral chi-square random variables with 2 degree of freedom [26], the order mismatch probability P_e can be calculated as

$$\begin{aligned} P_e = {} & Q_1\left(\frac{\sqrt{2}\left|\hat{H}_T(j)\right|}{\sigma_{TR}}, \frac{\sqrt{2}\left|\hat{H}_T(i)\right|}{\sigma_{TR}}\right) \\ & - \frac{1}{2} e^{\left[-\frac{|\hat{H}_T(i)|^2+|\hat{H}_T(j)|^2}{\sigma_{TR}^2}\right]} I_0\left(\frac{2\left|\hat{H}_T(i)\right|\left|\hat{H}_T(j)\right|}{\sigma_{TR}^2}\right), \end{aligned} \tag{25}$$

where $Q_\theta(a,b)$ denotes the Marcum Q-function, that is

$$Q_\theta(a,b) = \int_b^\infty x\left(\frac{x}{a}\right)^{\theta-1} e^{-\frac{x^2+a^2}{2}} I_{\theta-1}(ax)\,dx. \tag{26}$$

Let D denote the observed channel gain difference between subcarriers i and j at the transmitter, i.e., $|\hat{H}_T(i)|^2 = |\hat{H}_T(j)|^2 + D$, then P_e can be rewritten as

$$\begin{aligned} P_e = {} & Q_1\left(\frac{\sqrt{2}\sqrt{\left|\hat{H}_T(i)\right|^2 - D}}{\sigma_{TR}}, \frac{\sqrt{2}\left|\hat{H}_T(i)\right|}{\sigma_{TR}}\right) \\ & - \frac{1}{2} e^{\left[-\frac{2|\hat{H}_T(i)|^2-D}{\sigma_{TR}^2}\right]} I_0\left(\frac{2\left|\hat{H}_T(i)\right|\sqrt{\left|\hat{H}_T(i)\right|^2 - D}}{\sigma_{TR}^2}\right). \end{aligned} \tag{27}$$

As indicated in (27), the order mismatch probability P_e is determined by the channel gain $|\hat{H}_T(i)|^2$, channel gain difference D, and noise power σ_{TR}^2. A look-up table for D under various channel conditions with different order mismatch probabilities P_e can be generated from (27), as illustrated in Table I. Given a constraint on the order mismatch probability of two adjacent interleaved subcarriers, denoted by Λ, the required channel gain difference D under a given channel condition can be determined and utilized as a criterion to choose the interleaved subcarriers.

C. Interleaved Subcarrier Selection Procedure

In the proposed eavesdropping-resilient OFDM system, interleaved subcarriers are selected with constraints Ω and Λ. Ω determines the minimum number of interleaved subcarriers, while Λ determines which subcarriers are going to be interleaved. It is noteworthy that when we select the subcarriers according to the constraint Λ, the size of the set of qualified subcarriers, M, may be smaller than M_{min} under certain channel conditions. As an eavesdropping-resilient system, it should first ensure the protection against eavesdropping, and then mitigate the side-effects on the legitimate transmission. The subcarrier selection should thus give higher priority to the M_{min} requirement. In the case where $M < M_{min}$, the order mismatch criterion Λ has to be relaxed to include more subcarriers in the interleaving operation.

TABLE I
LOOK-UP TABLE FOR INTERLEAVED SUBCARRIER SELECTION WITH $P_e = 0.01$

$\left\|\hat{H}_T(i)\right\|^2$	$10\log_{10}\left(1/\sigma_{TR}^2\right)$ dB															
	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
0.02	0.040	0.030	0.025	0.020	0.015	0.010	0.010	0.010	0.005	0.005	0.005	0.005	0.005	0.005	0.005	0.005
0.04	0.080	0.060	0.045	0.035	0.030	0.020	0.020	0.015	0.010	0.010	0.010	0.005	0.005	0.005	0.005	0.005
0.06	0.120	0.090	0.070	0.055	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010	0.010	0.005	0.005	0.005
0.08	0.160	0.120	0.090	0.070	0.055	0.040	0.035	0.025	0.020	0.015	0.015	0.010	0.010	0.010	0.005	0.005
0.10	0.200	0.150	0.115	0.085	0.065	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010	0.010	0.005
0.12	0.240	0.180	0.135	0.105	0.080	0.060	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010	0.010
0.14	0.280	0.210	0.155	0.120	0.090	0.070	0.055	0.045	0.035	0.030	0.025	0.020	0.015	0.010	0.010	0.010
0.16	0.320	0.235	0.180	0.135	0.105	0.080	0.065	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010
0.18	0.355	0.265	0.200	0.155	0.115	0.090	0.070	0.055	0.045	0.035	0.030	0.025	0.020	0.015	0.010	0.010
0.20	0.395	0.280	0.225	0.170	0.130	0.100	0.080	0.060	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010
0.40	-	-	0.445	0.335	0.260	0.200	0.155	0.120	0.095	0.075	0.060	0.050	0.040	0.030	0.025	0.020
0.60	-	-	-	-	0.385	0.300	0.230	0.180	0.140	0.110	0.090	0.070	0.055	0.045	0.035	0.030
0.80	-	-	-	-	-	0.395	0.305	0.240	0.190	0.150	0.115	0.095	0.075	0.060	0.045	0.040
1.00		-	-	-	-	0.495	0.385	0.300	0.235	0.185	0.145	0.115	0.090	0.075	0.060	0.045
1.20	-	-	-	-	-	-	0.460	0.360	0.280	0.220	0.175	0.140	0.110	0.085	0.070	0.055
1.40	-	-	-	-	-	-	-	0.420	0.325	0.255	0.205	0.160	0.125	0.100	0.080	0.065
1.60	-	-	-	-	-	-	-	0.475	0.375	0.295	0.230	0.185	0.145	0.115	0.090	0.075
1.80	-	-	-	-	-	-	-	-	0.420	0.330	0.260	0.205	0.160	0.130	0.100	0.080
2.00	-	-	-	-	-	-	-	-	0.465	0.365	0.290	0.230	0.180	0.145	0.115	0.090

The procedure of the proposed subcarrier selection algorithm can be summarized as follows:

1) The minimum number of subcarriers to be interleaved is calculated from (23) with a given constraint Ω;
2) All N subcarriers of an OFDM signal are arranged in descending order according to their channel gains;
3) The subcarrier with the largest channel gain is selected first;
4) With the channel gain of the previously selected subcarrier, the estimated noise power and the constraint Λ, the required channel gain difference between the previously selected subcarrier and next subcarrier, D, is updated by referring to Table I;
5) The subcarrier, which has a channel gain at least smaller by a value of D than that of the previously selected subcarrier while it is closest to the previously selected subcarrier among all the qualified subcarriers, is selected;
6) Steps 4 and 5 are repeated until reaching the end of the order of the N subcarriers. Then M out of the N subcarriers have been selected out;
7) If $M \geq M_{min}$, the subcarrier selection is completed; otherwise, one has to relax the requirement of Λ, and then repeats steps 4 and 5 until $M \geq M_{min}$ can be achieved. If M is still smaller than M_{min} after Θ iterations, M_{min} subcarriers are selected from the N ordered subcarriers with an equal index interval, and then the selection procedure ends.

VI. SIMULATION RESULTS

Monte Carlo simulations are carried out following the specifications of IEEE 802.11g standard [27]. OFDM signals are generated using 64-point IFFT with a cyclic prefix (CP) of length 16. The modulation scheme quadrature phase-shift keying (QPSK) is adopted for all subcarriers. A rate 1/2 convolutional encoder with generator polynomials $[133_8, 171_8]$ and Viterbi decoder are also included in the simulations. For the interleaved subcarrier selection, Ω is set to 0.01 while Λ varies between 0.01 and 0.001. Unless stated otherwise, the subcarrier selection result ξ is assumed to be known by both the legitimate receiver and eavesdropper. In addition, the eavesdropper is assumed to deduce the interleaving pattern from its own channel estimate, i.e., the estimate of the eavesdropping channel.

Rayleigh fading channels with both uniform and exponential power delay profiles (PDP) are considered in the simulations. The channels are set to be time invariant over several data blocks, so that the transmitter and legitimate receiver are able to have channel estimates of identical channels. To make fair comparisons, we assume that the main channel and eavesdropping channel follow an identical statistical model, and that the noise levels at all nodes are the same. The least-square channel estimation technique is employed at all nodes in the network. Meanwhile, perfect synchronization is assumed at both the legitimate receiver and eavesdropper ends.

A. Evaluation of the CSI-Based Interleaving Permutation

1) Interleaving Permutation Mismatch Probability: The interleaving permutation mismatch probabilities at both the eavesdropper and legitimate receiver, which essentially determine the security and reliability of the proposed system, are evaluated in Fig. 3. A Rayleigh fading channel with uniform PDP of a delay spread as long as the CP length, i.e., 800 ns in the 802.11g system, is used in the simulations. As shown in the figure, the interleaving permutation mismatch probability at the eavesdropper is always close to 1 in the simulated channel conditions, whether $\Lambda = 0.01$ or $\Lambda = 0.001$. Accordingly, the information recovery for eavesdropping would be severely disrupted, which makes the transmitted data unrecognizable to the eavesdropper. In contrast, the interleaving permutation mismatch probability at the legitimate user is lower than 10^{-3} when SNR is larger than 15 dB. Since the interleaving permutation mismatch between legitimate users is mainly caused by channel estimation errors, a channel estimation technique inducing smaller estimation errors can further improve the reliability of the legitimate transmission.

2) Comparison With the CSI-Based Secret Key Generation Scheme: Similar to the proposed subcarrier interleaving scheme, CSI-based secret key generation schemes also exploit the randomness of wireless channels to protect the transmission.

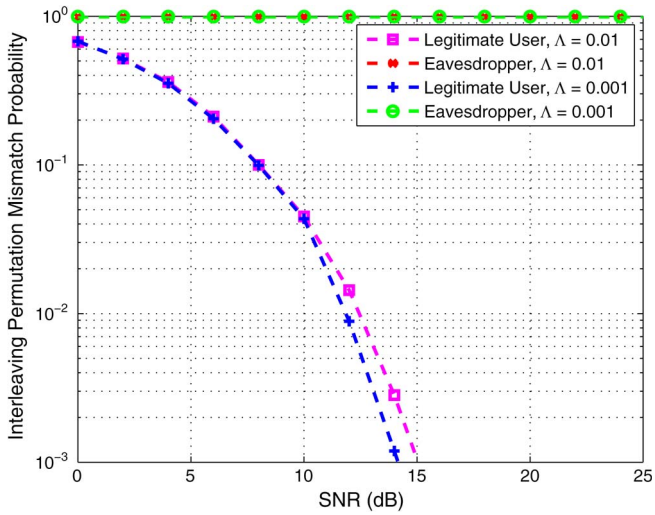

Fig. 3. Interleaving permutation mismatch probabilities at the legitimate receiver and eavesdropper ends.

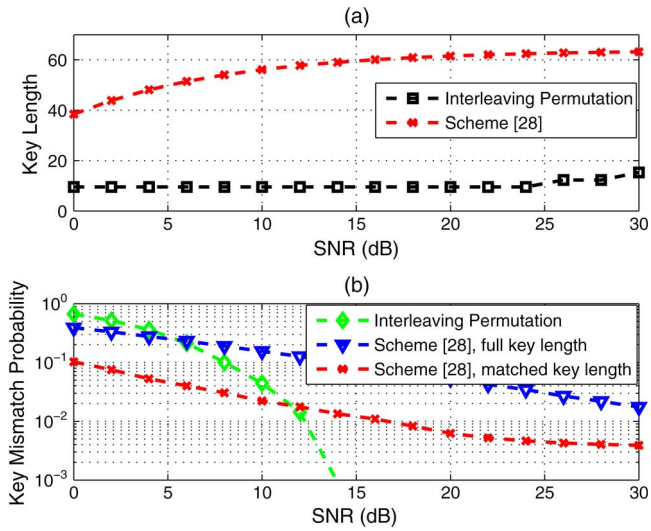

Fig. 4. Security and reliability comparison between the proposed interleaving permutation and the key generated by [28]. (a) Security comparison. (b) Reliability comparison.

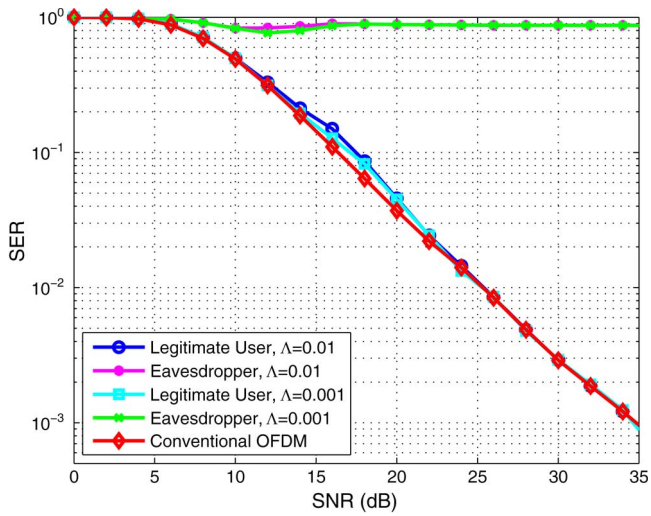

Fig. 5. SER vs. SNR under a Rayleigh fading channel with uniform PDP of 800 ns delay spread.

To some extent, the subcarrier interleaving permutation can be treated as a *secret key*. Therefore, it is interesting to compare the security and reliability achieved by the interleaving permutation and CSI-based secret keys.

Considering that the interleaving pattern in the proposed system is determined by subcarrier channel gains, a typical received signal strength (RSS) based secret key generation protocol [28] is adopted for this comparison. In [28], the RSS was compared with two reference thresholds q_+ and q_-. If RSS is larger than q_+, bit 1 is generated; if RSS is smaller than q_-, bit 0 is generated. Moreover, a key reconciliation technique was also introduced to mitigate its probability of key mismatch. Please refer to [28] for the detailed design.

The security of these two schemes is compared in terms of the length of generated "*keys*." With M involved subcarriers, the scheme in [28] can generate M bits of secret key, while the proposed subcarrier interleaving permutation can provide a "*key*" with a length of $\log_2(M!)$ bits. However, due to the subcarrier selection algorithm in the proposed system and the key reconciliation technique in [28], the numbers of subcarriers involved in the "*key*" generation under an identical channel condition may be different in the two schemes. The reliability of these two schemes is evaluated in terms of the "*key*" mismatch probability between the legitimate users. To remove the effect of the "*key*" length on the reliability comparison, the mismatch probability of a key generated by [28] with the same length as that from the subcarrier interleaving scheme is also provided. Comparison results are shown in Fig. 4. Under an identical channel condition, the key generated by [28] can have a longer length, while the "*key*" from the interleaving permutation is significantly more reliable. Therefore, the preferred method depends on the actual "*key*" length and reliability requirements.

B. Performance of the Proposed Secure OFDM System

In the simulations, the performance of the proposed secure OFDM system is evaluated from SERs experienced by the legitimate receiver and eavesdropper. The SER of the conventional OFDM system is provided as a bench-mark reference to assess the transmission reliability of the proposed system.

Fig. 5 shows the SERs of the proposed and conventional OFDM systems under a Rayleigh fading channel with uniform PDP of 800 ns delay spread. It can be observed from this figure that an eavesdropper always has a SER close to 1 when it utilizes its local channel estimates to intercept signals transmitted from the proposed OFDM system. In contrast, the performance of the legitimate transmission can be almost the same as that of the conventional OFDM system. In the simulated rich multipath environment, the maximum transmission reliability degradation of the proposed system when $\Lambda = 0.01$ and $\Lambda = 0.001$ is only 0.039 and 0.018, respectively, compared with the conventional OFDM system.

The SER vs. SNR performance of the proposed secure OFDM system under a different channel condition is depicted in Fig. 6, where a Rayleigh fading channel with exponential PDP of 50 ns root-mean-square (RMS) delay spread is considered. This represents a multipath channel with much less scattering in comparison with the one used before. As illustrated in

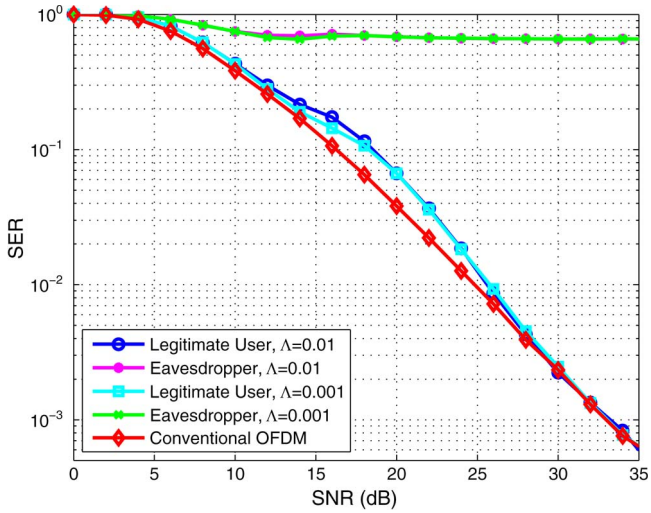

Fig. 6. SER vs. SNR under a Rayleigh fading channel with exponential PDP of 50 ns RMS delay spread.

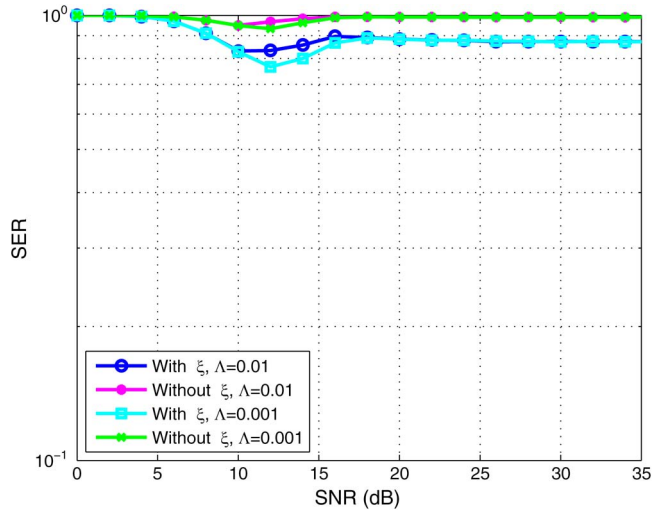

Fig. 7. SER comparison for eavesdroppers with and without the side information ξ in a Rayleigh channel with uniform PDP.

this figure, the eavesdropper still suffers from a very high SER though the SER is slightly less than that observed in Fig. 5. The SER of eavesdropping on the proposed system can be up to 506 times larger than that of eavesdropping on the conventional OFDM system in this simulated channel condition. Comparing the transmission reliability of the proposed OFDM system with that of the conventional OFDM system under the same channel condition, legitimate users in the proposed system would now experience a SER increase, which can be 0.067 at most when SNR $= 16$ dB and $\Lambda = 0.01$. However, by using a smaller Λ in the selection of interleaved subcarriers, the legitimate receiver can obtain a lower SER, such that the SER gap between the proposed and conventional OFDM systems can be reduced.

Comparing the performance results under different Rayleigh fading channel conditions, as shown in Figs. 5 and 6, the performance degradation of the proposed eavesdropping-resilient OFDM system can be explained as follows: the reciprocity and spatial variation properties of time-varying wireless channels, which are the basic principles behind the design, are more effective and reliable in rich multipath environments. Therefore, a rich scattering multipath environment is highly favorable to the proposed secure OFDM system.

C. Impact of Side Information ξ on Eavesdropping Prevention

The impact of the side information ξ on the eavesdropping prevention capability of the proposed OFDM system is also assessed. SERs at eavesdroppers with and without the knowledge of ξ under the Rayleigh fading channel with uniform PDP of 800 ns delay spread are compared in Fig. 7. In the simulations, the eavesdropper without the side information ξ would estimate the subcarrier selection based on its own channel observations, following the proposed subcarrier selection algorithm.

As shown in Fig. 7, the eavesdropper without information on ξ does experience higher SERs, compared with the one who knows exactly the interleaved subcarrier selection. The maximum security loss can be observed when SNR equals to 12 dB, where the SER decreases are 0.134 when $\Lambda = 0.01$ and 0.167 when $\Lambda = 0.001$, respectively. However, the SERs of eavesdropping are all considerably high, even when eavesdroppers can intercept, by chance, the side information ξ. Eavesdropping to the proposed system is always difficult. The reason of this phenomenon is that the eavesdropping prevention capability of the proposed system is dominated by the interleaving permutation itself instead of the side information ξ.

In addition, it can be observed from Fig. 7 that there is a small fluctuation in the eavesdroppers' SER values over the observed SNR range. This phenomenon is caused by the variation of the size of the interleaved subcarrier subset, i.e., M. The number of selected subcarriers varies according to channel conditions, and this directly affects the SER of eavesdropping as indicated in (10).

VII. Concluding Remarks

In this paper, we propose an eavesdropping-resilient OFDM system achieved by dynamic subcarrier interleaving. Exploiting the CSI between the transmitter and legitimate receiver, some subcarriers of each OFDM signal are selected and then interleaved according to the sorted order of their channel gains. Since wireless channels associated with each pair of users at separate locations exhibit independent fading processes, the frequently updated subcarrier interleaving pattern can only be shared between legitimate nodes based on channel reciprocity. Without a proper de-interleaving pattern, mismatched information recovery occurs at the eavesdropper, thus preventing eavesdropping. To mitigate the impairments from imperfectly reciprocal channel estimates at legitimate parties, interleaved subcarriers are selected according to a specially developed procedure to achieve a trade-off between the eavesdropping resilience and transmission reliability. Theoretical analysis and Monte Carlo simulation results have been provided to validate the proposed system. It can be observed from the simulation results that eavesdropping on the proposed system suffers from SER values close to 100% while the legitimate transmission has a SER performance about the same as that of conventional OFDM systems.

REFERENCES

[1] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[2] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[3] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and H. M. Salgado, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[6] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–5698, Oct. 2008.

[7] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[9] 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.

[10] Z. Gao, Y. H. Yang, and K. J. R. Liu, "Anti-eavesdropping space-time network coding for cooperative communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3898–3908, Nov. 2011.

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

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

[13] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.

[14] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[15] A. Chorti and H. V. Poor, "Faster than nyquist inference assisted secret communication for OFDM systems," in *Proc. IEEE Asilomar Conf. Signals, Syst. Comput.*, 2011, pp. 183–187.

[16] W.-J. Lin and J.-C. Yen, "An integrating channel coding and cryptography design for OFDM based WLANs," in *Proc. IEEE Int. Symp. Consum. Electron.*, 2009, pp. 657–660.

[17] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in TDS-OFDM system using constellation rotation and noise insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328–1332, Aug. 2010.

[18] H. Li, X. Wang, and Y. Zou, "Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1059–1062, Jun. 2014.

[19] W. Y. Zou and Y. Wu, "COFDM: An overview," *IEEE Trans. Broadcast.*, vol. 41, no. 1, pp. 1–8, Mar. 1995.

[20] S.-W. Lei and V. K. N. Lau, "Performance analysis of adaptive interleaving for OFDM systems," *IEEE Trans. Vel. Technol.*, vol. 51, no. 3, pp. 435–444, May 2002.

[21] A. Filippi and E. Costa, "Low-complexity interleaved subcarrier allocation in multicarrier multiple-access systems," *IEEE Trans Commun.*, vol. 55, no. 1, pp. 35–39, Jan. 2007.

[22] S. Mathur *et al.*, "Exploiting the physical layer for enhanced security," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, Oct. 2010.

[23] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 2, pp. 18–48, 2007.

[24] United states computer emergency readiness team (2012, Jan. 06), Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack. [Online]. Available: http://www.us-cert.gov/ncas/alerts/TA12-006A

[25] H. A. David, *Order Statistics*. New York, NY, USA: Wiley, 1981.

[26] M. K. Simon and M.-S. Alouini, "On the difference of two chi-square variates with application to outage probability computation," *IEEE Trans. Commun.*, vol. 49, no. 11, pp. 1946–1954, Nov. 2001.

[27] *IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, 2012.

[28] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. ACM Int. Conf. Mobile Comput. Netw.*, Sep. 2008, pp. 128–139.

Hao Li received the B.E. degree in measurement and control technology from University of Electronic Science and Technology of China, Chengdu, China, in 2008, and the M.E.Sc. and Ph.D. degrees in electrical and computer engineering from University of Western Ontario, London, ON, Canada, in 2010 and 2013, respectively. He is currently a Research Engineer in the Innovation Centre for Information Engineering, University of Western Ontario, London, ON. His research interests include the areas of communications and signal processing, with emphasis on adaptive and secure wireless communications, 5G communication systems, positioning, and signal estimation and detection.

Xianbin Wang (S'98–M'99–SM'06) received the Ph.D. degree in electrical and computer engineering from National University of Singapore, Singapore, in 2001.

Prior to joining Western University, he was a Research Scientist/Senior Research Scientist with the Communications Research Centre Canada from July 2002 to December 2007. From January 2001 to July 2002, he was a System Designer at STMicroelectronics, where he was responsible for system design for DSL and Gigabit Ethernet chipsets. He is a Professor at Western University and Canada Research Chair in Wireless Communications. His current research interests include adaptive wireless systems, 5G networks, communications security, and distributed computing systems. He has 200 peer-reviewed journal and conference papers on various communication system design issues, in addition to 24 granted and pending patents and several standard contributions.

Dr. Wang is an IEEE Distinguished Lecturer. He was the recipient of three IEEE Best Paper Awards. He currently serves as an Associate Editor for IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE TRANSACTIONS ON BROADCASTING. He was also an editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS between 2007 and 2011. He was involved in a number of IEEE conferences including GLOBECOM, ICC, WCNC, VTC, ICME and CWIT, in different roles such as symposium chair, tutorial instructor, track chair, TPC and session chair.

Jean-Yves Chouinard is a Professor with the Department of Electrical and Computer Engineering, Université Laval, Quebec City, QC, Canada. His research interests are wireless communications, secure communication networks and signal processing for radar applications. He is the author/co-author of more than 200 journal, conference papers and technical reports. He was co-recipient of the 1999 Neal Shepherd Best Propagation Paper Award from the IEEE Vehicular Society and of the 2004 Signal Processing Best Paper Award from the European Journal of Signal Processing. He is an editor of a book on information theory and co-author of book chapters on MIMO wireless communication systems and on OFDM-based mobile broadcasting. He is an Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY AND ASSOCIATE EDITOR for the IEEE TRANSACTIONS ON BROADCASTING. He has served on several conference committees including Technical Program Co-chair for the 2012 Vehicular Technology Conference (VTC'2012 Fall) and Publications Chair for the IEEE International Symposium on Information Theory (ISIT'2008).