Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 1 (2016), pp. 453-461

http://www.ripublication.com

Prevention of Eavesdropping in OFDMA Systems

R. Raja Kumar
Professor, Department of Mathematics,
Sathyabama University, Chennai-600119, India.

Abstract

In this paper, a novel anti-eavesdropping OFDM system through dynamic subcarrier coordinate interleaving is proposed by exploiting the reciprocal, location-dependent and time-varying nature of wireless channels. The transmitter performs coordinate interleaving at some of the OFDM subcarriers in an opportunistic manner, where the secret interleaving pattern is determined by the instantaneous channel state information (CSI) between the transmitter and intended receiver. More specifically, a subcarrier symbol associated with a channel phase larger than a predefined threshold is coordinate interleaved. Since wireless channels associated with each pair of users at separate locations exhibit independent multipath fading, the frequently updated coordinate interleaving pattern can only be shared between legitimate users based on channel reciprocity. Consequently, eavesdropping is prevented due to mismatched de-interleaving at the eavesdropper. Theoretical analysis and simulation results are provided to validate the proposed system.

Keywords: Physical layer security, OFDM, eavesdropping prevention, coordinate interleaving.

Introduction

Orthogonal Frequency-Division Multiplexing (OFDM) has been widely employed in modern wireless communications networks. Unfortunately, conventional OFDM signals are vulnerable to malicious eavesdropping due to their distinct time and frequency characteristics. As the physical-layer transmission parameters of OFDM signals can be blindly estimated by adversaries, traditional upper-layer security mechanisms cannot completely address security threats in wireless OFDM systems. Physical layer security, which targets communications security at the physical layer, is emerging as an effective complement to traditional security strategies in securing wireless OFDM transmission [1]. The physical layer security of OFDM systems over

wireless channels was investigated from an information-theoretic perspective in [1]. Based on the theoretical secrecy capacity study, several OFDM security techniques have been proposed. A secure OFDM system was investigated by degrading the eavesdropper's channel condition, where distributed transmitters independently sent out pre-equalized OFDM signals [2]. Power and subcarrier allocation schemes in OFDM systems subject to the power and security constraints were reported in [3]. Moreover, transmit beamforming [4],artificial noise [5] and cooperation transmission [6] can also be adopted to improve the security of OFDM-based transmission. However, these secretive capacity based security techniques usually require the knowledge of the eavesdropping channel, which is conditioned on a successful detection of eavesdroppers. Also, additional resource may be needed like cooperative terminals and multiple antennas. Simple proactive eavesdropping prevention for OFDM at the physical layer, without significant modifications to off-the-shelf systems, has yet to be developed. The concept of coordinate interleaving was originally introduced into communications systems to improve the reliability of data transmission [7], and later extended to space-time code designs for multiple-input multiple-output transmission [8]. In[9], a coordinate interleaving method was utilized to decrease the error rate in cooperative relay networks. However, none of these works take into account security issues. In this paper, we propose a simple and effective anti-eavesdropping OFDM system, by exploiting dynamic coordinate interleaving at a subset of OFDM subcarriers. Technically, the transmitter interleaves the real and imaginary components of a subcarrier symbol when its associated channel phase is larger than a predefined threshold. Based on channel reciprocity, the legitimate receiver can locally deduce subcarriers that undergo coordinate interleaving without any additional signaling. In contrast, due to the independence of spatially separate wireless channels in a rich multipath environment, the subcarrier coordinate interleaving pattern is unavailable to the eavesdropper at a third location. Consequently, de-interleaving at the eavesdropper is disrupted and eavesdropping is then prevented. Compared with existing security approaches, the proposed scheme guarantees computational security without any requirement of eavesdropping channel information, secret information exchange or special cipher processing. In addition, it only needs minor modifications to off-the-shelf systems, and has low computational complexity.

II. SYSTEM MODEL AND PRELIMINARIES

A. System Model

Consider an OFDM wireless network that consists of three nodes: a transmitter communicates with a legitimate receiver in the presence of a passive eavesdropper. The eavesdropper knows the security protocol of the legitimate transmission and has the capability to demodulate OFDM signals. It can intercept all communications between legitimate users but is unable to wiretap their inside processing like channel estimations. The forward and reverse channels between legitimate users are assumed to occupy the same frequency band and remain constant over several time slots. Hence, the transmitter and legitimate receiver would experience and observe an identical main channel based on the reciprocity property of wireless channels. Meanwhile, the

eavesdropper is assumed to be spatially separated from the legitimate users with more than half a wavelength, which means that the main channel and eavesdropping channel are independent of each other.

B. Multipath Channels in OFDM System

Assume that OFDM signals with N subcarriers are transmitted by the transmitter. At the legitimate receiver, the frequency domain received signals after removing the cyclic prefix, $\mathbf{R} = [R(0); R(1); \cdots; R(N-1)]^T$, can be written as

$$\mathbf{R} = \text{diag}\{\mathbf{H}\}^N\mathbf{S} + \mathbf{W}; \quad (1)$$

Where $\text{diag}\{\mathbf{H}\}^N$, which is an $N \times N$ diagonal matrix with all its main diagonal entries $\mathbf{H}=[H(0); H(1); \cdots; H(N-1)]^T$, identifies the complex frequency domain channel responses of the main channel; $N \times 1$ vector $\mathbf{S}$ denotes modulated symbols transmitted by the N subcarriers, which are mapped into a two-dimensional constellation; and vector $\mathbf{W}$ of size $N \times 1$indicates the white Gaussian noise following the distribution $CN(0; \sigma^2_w)$. Throughout the analysis, we approximate the N subcarrier channels as independent and identically distributed (i.i.d.) random variables following the distribution $CN(0;\sigma^2_H)$.The same modelling and approximation can be applied to the analysis of the eavesdropping channel $\mathbf{H_E}$. Similarly, $\{H_E(0); H_E(1); \cdots; H_E(N-1)\}$ are modelled as i.i.d. complex Gaussian variables distributed as $CN(0;\sigma^2_{HR})$.

C. Channel Estimates in the Network

Estimation errors generally occur at channel estimators, due to the presence of noise, interference and hardware limitations in wireless communications systems. As a result, only noisy channel estimates can be obtained by all nodes in the network. The observations of the main channel at the transmitter and legitimate receiver,

$$\left|\hat{H}_{T/R}(k)\right| e^{j\hat{\theta}_{T/R}(k)} = \left|H(k)\right| e^{j\theta(k)} + \left|\Delta H_{T/R}(k)\right| e^{j\Delta\theta_{T/R}(k)} \quad (2)$$

where subscripts T and R indicate variables associated with the transmitter and legitimate receiver, respectively. $|\cdot|$indicates the norm operation; $\hat{\Theta}_{T/R}(k)$ denotes the estimated channel phase at the k the subcarrier of the main channel while $\Theta(k)$ is its exact value; and $\Delta\Theta_{T/R}(k)$ represents the phase of the estimation error $\Delta H_{T/R}(k)$. Similarly, the estimate of the eavesdropping channel at the eavesdropper can be given by

$$\left|\hat{H}_E(k)\right| e^{j\hat{\theta}_E(k)} = \left|H_E(k)\right| e^{j\theta_E(k)} + \left|\Delta H_E(k)\right| e^{j\Delta\theta_E(k)}, \quad (3)$$

Where $\hat{\Theta E}(k)$, $\Theta_E(k)$ and $\Delta\Theta_E(k)$ denote the phases of the estimated channel response $\hat{HE}(k)$, the eavesdropping channel $HE(k)$, and the estimation error $\Delta HE(k)$, respectively.

OFDM with Dynamic Coordinate Interleaving

In the proposed OFDM system, a subcarrier set M with M out of the N subcarriers in each OFDM signal is involved in the dynamic coordinate interleaving, where whether

the symbol coordinate at a subcarrier is interleaved is determined by the instantaneous subcarrier channel state information (CSI).In this paper, a channel phase based interleaving pattern generation scheme is adopted as an example to demonstrate how the dynamic coordinate interleaving can prevent eavesdropping.

A. Transmitter End in the Proposed Secure OFDM System

At the transmitter end, the instantaneous channel phase of each subcarrier belonging to set M in an OFDM signal is compared with a properly selected threshold Λ_T. If the channel phase of a subcarrier is larger than the threshold, the real and imaginary components of the symbol at that subcarrier are interleaved (In case that the real and imaginary components are identical, their signs are reversed). Otherwise, the modulated symbol at that subcarrier is transmitted in the original format. The other processing of the transmitter is the same as that of a conventional OFDM transmitter. Mathematically, the channel phase based coordinate interleaving pattern can be written as

$$\begin{cases} \hat{\theta}_T(k) > \Lambda_T, & \text{interleaving} \\ \hat{\theta}_T(k) \le \Lambda_T, & \text{un-interleaving} \end{cases}, \quad k \in \mathcal{M}. \tag{4}$$

As the noisy channel estimate ^**HT** follows a zero-mean complex Gaussian distribution $CN(0;\sigma^2_{HT})$, the estimated phases of the N subcarriers in an OFDM signal, $\{\hat{\Theta}T(0); \hat{\Theta}T(1); \cdots; \hat{\Theta}T(N-1)\}$, are i.i.d. variables uniformly distributed over $(0; 2\_]$. In order to maximize the difficulty of eavesdropping, an OFDM subcarrier should have an equal probability of being and not being coordinate interleaved. Therefore, the threshold ΛT can be selected as: $\Lambda T = \pi$.

B. Receiver End in the Proposed Secure OFDM System

Compared with a conventional OFDM receiver, the only difference of the receiver in this system is that a coordinated e-interleaving is carried out at subcarriers in set M after the symbol demodulation. The receiver would locally determine the de-interleaving pattern by comparing its observation $\hat{\Theta}R(k)$ with a predefined threshold ΛR, where $k \in M$. Since ^$\mathbf{H_R}$ follows a zero-mean complex Gaussian distribution $CN(0; \hat{\sigma}_{HR})$, the corresponding subcarrier channel phases$\{\hat{}_R(0); \hat{}_R(1); \cdots; \hat{}_R(N-1)\}$are i.i.d. variables uniformly distributed over $(0; 2\_]$. Thus, ΛR should also be π.

IV. PERFORMANCE EVALUATION

A. SERs of Eavesdropping and Legitimate Transmission Eavesdropping:

Since the eavesdropper at a third location experiences a multipath channel independent of the main channel, the subcarrier channel phase estimate at the eavesdropper, ^Θ**E**, is uncorrelated to that observed at the transmitter, i.e. ^Θ**T**. Hence, the eavesdropper can only make a random guess of the time-varying coordinate interleaving pattern initiated by the transmitter. As a binary hypothesis problem where both possible outcomes have the same occurrence probability, the probability that the eavesdropper makes a correct decision of whether the modulated symbol at a subcarrier in set M is coordinate interleaved would be 1/2. When M subcarriers are involved in the opportunistic coordinate interleaving, the probability that the eavesdropper obtains a mismatched interleaving pattern for an OFDM signal, P_E, can be calculated as

$$P_E = 1 - \frac{1}{2^M}. \tag{5}$$

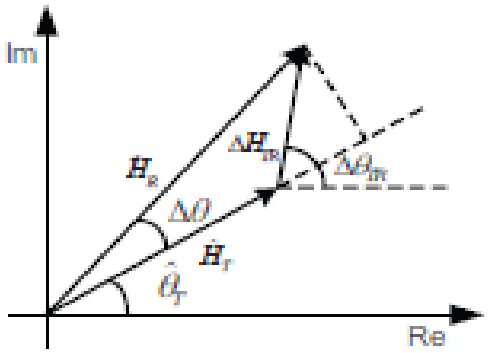

Figure 1: Derivation of the phase estimation error from noisy channel estimates.

Let *PS* denote the symbol error rate (SER) of the conventional OFDM system using a certain modulation scheme in a multipath fading channel. The SER of eavesdropping to the proposed OFDM system, $P_{S;E}$, can be given by

$$P_{S;E} = 1 - (1 - P_E)(1 - P_S), \tag{6}$$

Legitimate Transmission: The probability that the two end nodes of the main channel disagree on whether a subcarrier in set *M* is coordinate interleaved, $p_L(k)$, can be derived as

$$\begin{aligned} p_L(k) &= \frac{1}{2}P\left(\hat{\theta}_R(k) > \pi, \hat{\theta}_T(k) \le \pi\right) \\ &\quad + \frac{1}{2}P\left(\hat{\theta}_R(k) \le \pi, \hat{\theta}_T(k) > \pi\right). \end{aligned} \tag{7}$$

The subcarrier channel phase estimates at the transmitter and legitimate receiver, i.e. $\hat{\Theta}\mathbf{T}$ and $\hat{\Theta}\mathbf{R}$, respectively, are conditioned on the exact phase of the main channel Θ. As a result, we can treat $\hat{\Theta}R(k)$ as a noisy version of $\hat{\Theta}T(k)$ for all *N* subcarriers of an OFDM signal, that is

$$\hat{\theta}_R(k) = \hat{\theta}_T(k) + \Delta\theta(k), \quad k = 0, 1, \cdots, N-1, \tag{8}$$

Where $\Delta\Theta(k)$ is the phase estimation error between estimates $\hat{\Theta}R(k)$ and $\hat{\Theta}T(k)$. As illustrated in Fig. 1, $\Delta\Theta(k)$ can be derived from the noisy channel estimate and approximated as

$$\Delta\theta(k) \approx \frac{\left|\Delta H_{TR}(k)\right| \sin\left[\Delta\theta_{TR}(k) - \hat{\theta}_T(k)\right]}{\left|\hat{H}_T(k)\right|}. \tag{9}$$

Referring to the statistics study in [10], the numerator of (9) follows a zero-mean Gaussian distribution with variance $\sigma^2 T/R/2$. Meanwhile, the denominator, $|\hat{H}_T(k)|$ is Rayleigh distributed with parameter $\sqrt{\sigma^2 HT/2}$. As a ratio between a zero-mean Gaussian

variable and a Rayleigh variable, $\Delta\Theta(k)$ has a probability density function (PDF), $f_\Theta(\Delta\Theta(k))$, as

$$f_\theta\left(\Delta\theta(k)\right) = \frac{\sigma_{TR}^2 \sigma_{\hat{H}_T}}{2\left(\sigma_{\hat{H}_T}^2 \Delta\theta(k)^2 + \sigma_{TR}^2\right)^{3/2}}. \tag{10}$$

The probability of disagreement between the transmitter and legitimate receiver on whether the kth subcarrier is coordinate interleaved, $p_L(k)$, can then be derived as

$$\begin{aligned} p_L(k) &= \frac{1}{2}\int_0^{\pi}\left[\int_{\pi-\hat{\theta}_T(k)}^{2\pi-\hat{\theta}_T(k)} f_\theta\left(\Delta\theta(k)\right)d\Delta\theta(k)\right]\frac{1}{2\pi}d\hat{\theta}_T(k) \\ &\quad + \frac{1}{2}\int_{\pi}^{2\pi}\left[\int_{-\hat{\theta}_T(k)}^{\pi-\hat{\theta}_T(k)} f_\theta\left(\Delta\theta(k)\right)d\Delta\theta(k)\right]\frac{1}{2\pi}d\hat{\theta}_T(k) \\ &= \frac{\sqrt{\sigma_{\hat{H}_T}^2 4\pi^2 + \sigma_{TR}^2} + \sigma_{TR} - 2\sqrt{\sigma_{\hat{H}_T}^2 \pi^2 + \sigma_{TR}^2}}{4\pi\sigma_{\hat{H}_T}}. \end{aligned} \tag{11}$$

When M subcarriers are involved in the dynamic coordinate interleaving, the interleaving pattern mismatch probability between the legitimate users for an OFDM signal, P_L, is

$$P_L = 1 - (1 - p_L)^M, \tag{12}$$

Similarly, we can have the SER of legitimate transmission in the proposed anti-eavesdropping OFDM system as

$$P_{S,L} = 1 - (1 - P_L)(1 - P_S), \tag{13}$$

B. Information Leakage at the Eavesdropper

In the proposed system, the bit error rate (BER) of eavesdropping at each subcarrier of the OFDM signal can be approximated as

$$p_k \approx \begin{cases} \frac{1-1/2(1-P_S)}{\alpha}, & k \in \mathcal{M} \\ \frac{P_S}{\alpha}, & k \notin \mathcal{M} \end{cases}, \tag{14}$$

Where α denotes the number of bits per symbol at a 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, YE, can be derived as

$$\begin{aligned} I_k(Y_E;X) &= \mathrm{H}_k(Y_E) - \mathrm{H}_k(Y_E|X) \\ &= 1 + p_k\log_2 p_k + (1-p_k)\log_2(1-p_k). \end{aligned} \tag{15}$$

Where H(·) denotes the entropy operation.With respect to the whole OFDM signal with N independent subcarriers, the information leakage can be derived as

$$L_{OFDM} = \frac{1}{N}\sum_{k=0}^{N-1} I_k(Y_E;X), \tag{16}$$

Which can finally be given by (17).

$$L_{OFDM} = 1+(1-\frac{M}{N})\left[\frac{P_S}{\alpha}\log_2\frac{P_S}{\alpha}+(1-\frac{P_S}{\alpha})\log_2(1-\frac{P_S}{\alpha})\right]$$
$$+\frac{M}{N}\left[\frac{1+P_S}{2\alpha}\log_2\frac{1+P_S}{2\alpha}+(1-\frac{1+P_S}{2\alpha})\log_2(1-\frac{1+P_S}{2\alpha})\right] \quad (17)$$

C. Security against Brute Force Attacks

Under brute force attacks, it is true that the eavesdropper with unlimited power and storage can test all 2*M* permutations of each interleaving pattern and then retrieve the original signal. However, the proposed system can benefit from the continued influx of channel randomness and thus defend against brute force attacks. The coordinate interleaved pattern adopted by the transmitter is updated each channel coherence time. As long as the eavesdropper cannot break an interleaving pattern within such a time period, which is true in most practical scenarios, 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, particularly when many subcarriers are involved in the dynamic coordinate interleaving.

Simulation Results

Simulations are carried out following the specifications of IEEE 802.11g standard. 4-QAM is adopted as the modulation scheme for all subcarriers, and a Rayleigh fading channel with exponential power delay profile (PDP) of 50 *ns* root-meansquare (RMS) delay is considered in the simulations. In order to make a fair comparison, the statistical models of the main channel and eavesdropping channel, as well as the noise power levels at all nodes, are set to be the same. The SER of the proposed anti-eavesdropping OFDM system is evaluated in Fig. 2. The proposed system can prevent eavesdropping and at the same time provide a reliable legitimate transmission. As the performance loss of the legitimate transmission is mainly caused by channel estimation errors, a more reliable channel estimation can further improve the transmission reliability. The information leakage at the eavesdropper in the proposed and conventional OFDM systems is presented in Fig. 3. The proposed system can significantly decrease the information leakage at the eavesdropper, especially when more subcarriers in an OFDM signal are involved in the dynamic coordinate interleaving. Please note that the information leakage of the proposed system mainly comes from subcarriers that are not involved in the interleaving.

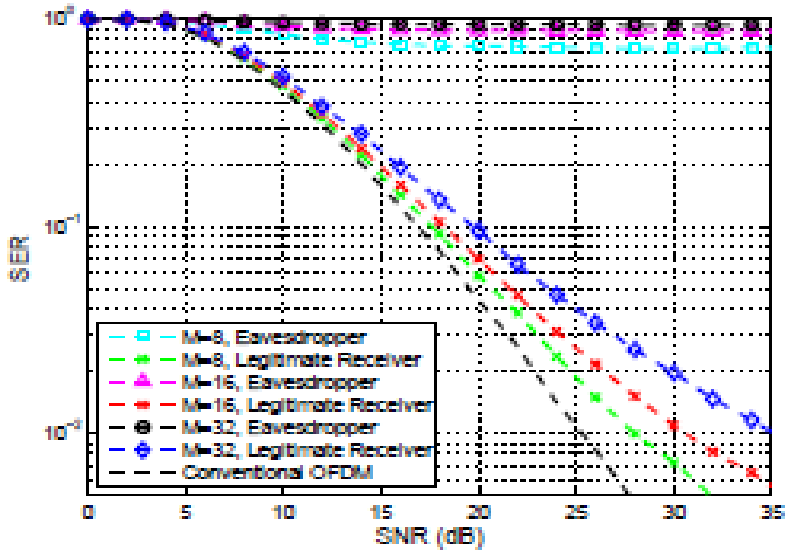

Figure 2: SER comparison between the proposed anti-eavesdropping OFDM system and convention DOFDM system

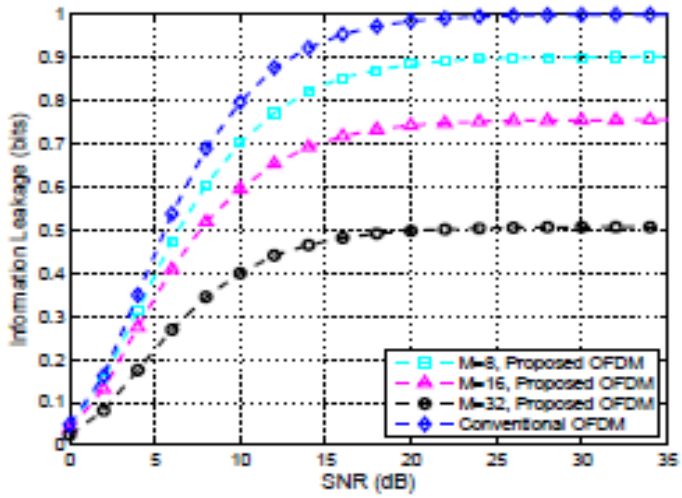

Figure 3: Information leakage at the eavesdropper in the proposed and conventional OFDM systems.

Conclusion

This paper proposed an eavesdropping prevention strategy in OFDM systems through dynamic subcarrier coordinate interleaving. Symbol coordinates at some subcarriers of each OFDM signal are interleaved in an opportunistic manner depending on the CSI between the transmitter and legitimate receiver. More specifically, the transmitter performs coordinate interleaving at subcarriers with channel phases larger than a predefined threshold. Since wireless channels associated with each pair of users at

separate locations exhibit independent propagation characteristics, the frequently updated coordinate interleaving pattern is only shared between legitimate users based on channel reciprocity. Without a matched coordinate de-interleaving pattern, erroneous information recovery is carried out at the eavesdropper so that eavesdropping is prevented. Theoretical analysis and simulation results have been provided to validate the proposed anti-eavesdropping OFDM system.

References

[1] F. Renna, N. Laurenti and H. V. Poor, 2012, "Physical-Layer Secrecy for OFDM Transmissions over Fading Channels, "*IEEE Trans. Inf. Forens. Security*, vol. 7, no. 4, pp. 1354-1367.

[2] A. Chorti and H. V. Poor, 2011, "Faster than Nyquist Interference Assisted Secret Communication for OFDM Systems, " in *Proc. IEEE Asilomar Conf. Signals, Systems and Comput.*, pp. 183-187.

[3] X. Wang, *et al.*, 2011 "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks, "*IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 693-702.

[4] H. M. Wang, Q. Yin, and X. G. Xia, 2012 "Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks, " *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3545.

[5] S. Goel and R. Negi, 2008, "Guaranteeing Secrecy Using Artificial Noise, " *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189.

[6] Z. Ding, *et al.*, 2012, "On the Application of Cooperative Transmission to Secrecy Communications, "*IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368.

[7] J. Boutros and E. Viterbo, 1998 "Signal Space Diversity: A Power and Bandwidth-Efficient Diversity Technique for Rayleigh Fading Channel, "*IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1453-1467.

[8] C. Yoon, H. Lee, and J. Kang, 2011, "Performance Evaluation of Space-Time Block Codes from Coordinate Interleaved Orthogonal Designs in Shadowed Fading Channels, "*IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 1289-1295.

[9] J. Harshan and B. S. Rajan, 2009, "Co-ordinate Interleaved Distributed Space-Time Coding for Two-Antenna-Relays Networks, "*IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1783-1791.

[10] Y. E. H. Shehadeh, O. Alfandi, and D. Hogrefe, 2012, "Towards Robust Key Extraction from Multipath Wireless Channels, "*IEEE J. Commun.Netw.*, vol. 14, no. 4, pp. 385-394.