Space-Frequency Grouping Based Key Extraction for MIMO-OFDM Systems

Ozan Alp Topal*, Güneş Karabulut Kurt*, Berna Özbek†

*Wireless Communications Research Laboratory
Department of Electronics and Communication Engineering Istanbul Technical University, Istanbul, Turkey
† Electrical and Electronics Engineering Department
Izmir Institute of Technology, Izmir, Turkey
{topalo, gkurt}@itu.edu.tr, bernaozbek@iyte.edu.tr

***Abstract*—Latest developments in wireless communication networks push the limits of conventional security methods. Security can be improved with a secret key that is dynamically generated based on the surrounding physical environment. With this objective, physical layer security approaches can be implemented by means of simple signal processing methods. In this paper, we propose novel key extraction approaches based on spatial and frequency characteristics of the wireless environment. In a 2×2 MIMO-OFDM system, low key disagreement rates and key error rates are observed, proving the potential of physical layer key extraction techniques.**

***Keywords*—MIMO-OFDM, physical layer security, key error rate, key disagreement rate, secret key extraction.**

I. Introduction

In wireless communication systems, radio waves are emitted into the air, so they are open to interception within the coverage area. This provides a potential for eavesdropping attacks and the associated security vulnerabilities in the physical layer (PHY). Conventional cryptography techniques rely on encryption/decryption mechanisms on higher levels of communication systems [1]. These mechanisms bring high-complexity which may not be applicable in some application scenarios such as ad-hoc networks. PHY security is proposed considering reduced complexity applications.

A class of PHY security approaches rely on secret key extraction. Secret key extraction in PHY exploits both the reciprocity principle and the randomness of the wireless channel. A wireless transmission medium is characterized by random, time-varying multipath fading parameters for each communication link between two devices, and therefore it is considered to be an important incidental source for key-based PHY security systems. The additional complexity of PHY key generation is low, given that the channel parameters need to be estimated to enable communication. Thus, a key extraction system, which has a low computational load and high efficiency, can be implemented with simple equipment. Keys are created dynamically as the channel conditions change within a short time interval.

To evaluate the performance of PHY security systems, different error performance metrics have been previously purposed [2]. Key disagreement rate (KDR) and key error rate (KER) are the most frequently used performance metrics. KDR shows the disagreement rate of raw bits in the keys, while KER indicates whether keys are matched on both nodes. These error rates can be decreased further by information reconciliation techniques [3].

In this work, we consider key extraction for PHY security in a 2×2 multi-input multi-output (MIMO) orthogonal frequency division multiplexing (OFDM) system. The applicability of PHY security on these systems has been examined in both theoretical and practical aspects [4], [5]. Our contributions in this work are listed below.

- Novel key extraction methods based on frequency and space grouping of the channel responses are proposed.
- The effect of correlation between frequency and space groups is analyzed.
- Different channel characteristics are compared by the means of KDR and KER.
- Software defined radio (SDR) based tests are conducted to measure KER and KDR performances in a 2×2 MIMO-OFDM system.

A. Related Works

In [6], secure Internet of Things (IoT) communication is aimed, where sources generate and transmit additional incorrect data symbols to confuse eavesdroppers. Receiver side can extract information by channel dependent key extraction. In [7], the receiver processes data with two different boards from a common antenna, allowing the measurement of different noise effects on simultaneously sampled data. It shows experimentally that difference in sampling time affect cross correlation and eventually reciprocity. [8] presents different methods in order to improve the channel reciprocity response quality such as interpolation, curve fitting, and Savitzky Golay filtering. In addition to channel reciprocity, the decorrelation methods are considered, including Karhunen-Loéve transform, discrete cosine transform, Haar transform, and Walsh-Hadamard transform. These improvements are shown to be effective on reducing the KER. In [9], zero reconciliation secret key extraction method is proposed for backscatter wireless communication. Using precoding and artificial jamming, active and passive attacks can be precluded efficiently in

This work has been supported by TUBITAK Project 114E626.

978-1-5386-2913-0/17/$31.00 ©2017 IEEE

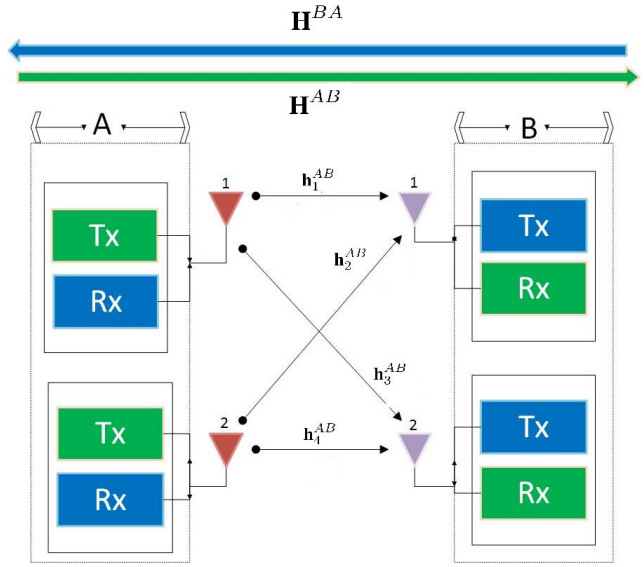

Figure 1: MIMO system model.

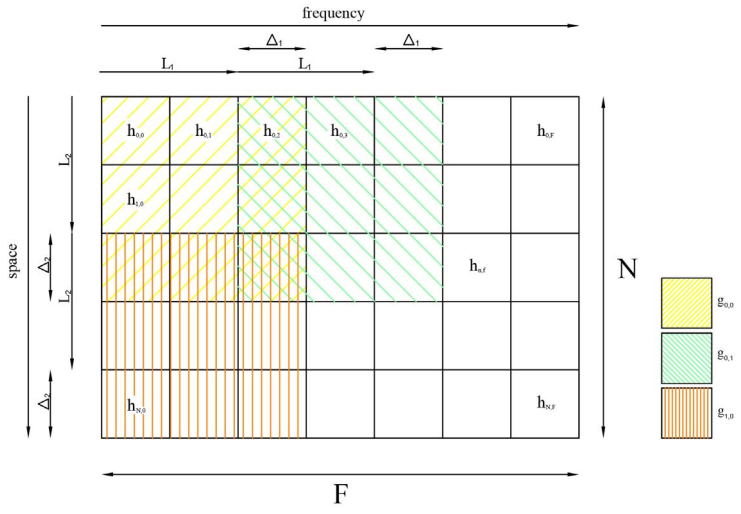

Figure 2: Space-frequency grouping model.

lower modulation orders. [10] presents performance results of key generation by enhancing channel reciprocity. Adaptive quantization technique is used for key generation.

II. System Model

The MIMO architecture is shown in Figure 1. Let F denote the number of subcarriers and N denote the number of antenna pairs. Assuming that the channel delay spread is shorter than the length of the cyclic prefix, the received symbols of the MIMO-OFDM system with N_t transmit antennas and N_r receive antennas can be modeled as

$$\mathbf{Y}^i = \mathbf{H}^i\mathbf{X}^i + \mathbf{W}^i \tag{1}$$

where $i \in \{AB, BA\}$, represents the transmission direction, from node A to node B or vice versa. $\mathbf{Y}^i \in \mathbb{C}^{N_r\times 1}$ is the received signal, $\mathbf{H}^i \in \mathbb{C}^{N_r\times N_t}$ is the channel matrix, $\mathbf{X}^i \in \mathbb{C}^{N_t\times 1}$ is the transmitted signal. $\mathbf{W}^i \in \mathbb{C}^{N_r\times 1}$ is the additive white Gaussian noise component with elements $\mathcal{CN}(0,\sigma^2)$. According to electromagnetic waves reciprocity [11], a reciprocal channel model implies $\mathbf{H}^{AB} = \mathbf{H}^{BA}$. Channel coefficient matrices are represented as $\mathbf{H}^{AB}$ and $\mathbf{H}^{BA}$. This equality may not hold because of RF front-end imperfections in practical systems.

III. Key Extraction Method

For an $N_t \times N_r$ MIMO-OFDM system, there are $N = N_tN_r$ reciprocal channel coefficient vector pairs $\mathbf{h}_n^i$ with length F. The channel coefficient from the n^{th} antenna pair and f^{th} subcarrier is represented as $h_{n,f}^{AB}$ and $h_{n,f}^{BA}$,where $f = 0, 1, \ldots, F-1$ and $n = 1, \ldots, N$ and $N = N_t \times N_r$. The amplitude ($|h_{n,f}^{AB}|$, $|h_{n,f}^{BA}|$) and phase ($\angle h_{n,f}^{AB}$, $\angle h_{n,f}^{BA}$) values of these channel coefficient vectors play an important role in key generation.

As it can be seen from Figure 2, we cluster channel matrix into groups which will be converted to key bits. In uncorrelated case, one subgroup $\mathbf{g}^i$ is consist of L_2 channel vectors with L_1 subcarriers.

We target to make use of correlation among the groups consisting of channel coefficients of subcarriers and antenna elements. In correlated case, channel coefficients can be grouped to be correlated to each other. Frequency correlation blocks are represented with Δ_1 while the spatial correlation blocks are represented with Δ_2.

After clustering channel coefficient matrix into subgroups, we follow two different methods to convert them to a security key. If we apply these methods separately to channel amplitudes and phases, we obtain four different scenarios. In first method, we use mean values of each subgroup for key extraction. It can be expressed as;

$$g_{n',f'}^i = \sum_{k=0}^{L_2+\Delta_2-1}\sum_{l=0}^{L_1+\Delta_1-1} w_{n,f}\mathrm{h}_{L_2n+k,L_1f+l}^i, \quad \text{for } n' = 0, ..., \left\lfloor\frac{N-\Delta_2}{L_2}\right\rfloor - 1;\ f' = 0, ..., \left\lfloor\frac{F-\Delta_1}{L_1}\right\rfloor - 1. \tag{2}$$

Subgroup $g_{n',f'}^i$ expresses mean value of $L_1+\Delta_1$ frequency and $L_2+\Delta_2$ spatial component. Therefore, $w_{n,f}$ weight vector can be selected as

$$w_{n,f} = \frac{1}{(L_1+\Delta_1)(L_2+\Delta_2)}. \tag{3}$$

For the second method, we use the maximum values of each subgroup for key extraction vector. It can be represent as;

$$g_{n',f'}^i = \max_{k\in\{0,...,L_2+\Delta_2-1\},l\in\{0,...,L_1+\Delta_1-1\}}\left(\mathrm{h}_{L_2n+k,L_1f+l}^i\right). \tag{4}$$

After converting series of subgroups to $\mathbf{g}^i$ vector; we can quantize the vectors considering all key extraction methods as;

$$\mathbf{K}^i = q(\mathbf{g}^i, M), \tag{5}$$

where $q(.)$ is the quantization function, M represents the number of bits for each quantized sample and $\mathbf{K}^i$ is the key of

the corresponding node ($\mathbf{K}^{AB}$ for node B and $\mathbf{K}^{BA}$ for node A). Then the overall key length becomes;

$$L = M.\left\lfloor \frac{N-\Delta_2}{L_2} \right\rfloor.\left\lfloor \frac{F-\Delta_1}{L_1} \right\rfloor. \tag{6}$$

Midrise type of uniform quantization method is applied to input vectors. Quantization process is described as follows. Firstly, the number of bits (M) for each quantized sample must be selected. This selection determines the number of quantization levels ($Q = 2^M$). Then, amplitude interval $\mathtt{A}$ has to be calculated from the maximum and the minimum values of vector which will be quantized. Step size (α) of quantizer must be computed from $\alpha = \mathtt{A}/Q$. After this process, the bits depend on M are assigned to each quantized sample. The generated bits are adjusted according to Gray code [12]. At the end of each method we obtain a code vector for both directions ($\mathbf{K}^{AB}$ and $\mathbf{K}^{BA}$). These vectors are compared by means of KDR and KER. KDR can be expressed as;

$$\text{KDR} = \frac{\sum_{j=1}^{L} |\mathbf{K}^{AB}(j) - \mathbf{K}^{BA}(j)|}{L}, \tag{7}$$

KER is a performance criterion which would be zero even one bit in the key mismatched; so for one key per user KER could be either 0 (mismatch) or 1 (match). It is effective when long key vectors are considered.

IV. Test Setup and Results

USRP NI-2921 kits are used as SDRs in the test environment. Measurements are made in ITU Electronics and Communication Engineering Department, Wireless Communications Research Laboratory. Software defined radio kits are programmed with LabVIEW software. USRP units are SDR kits and they contain an RF layer, analog-to-digital converter (ADC), digital-to-analog converter (DAC) and field programming gate array (FPGA) board. USRP units, which are very convenient for SDR applications, are flexible, high-speed and open source hardware. LabVIEW, which is used in many fields and has a library for each device, is the graphical programming language interface [13]. The testbed of the implementation of point to point MIMO-OFDM system is shown in Figure 3. Two USRPs are used as transmitter and two USRPs are used as receiver in the testbed, hence $N_t = N_r = 2$.

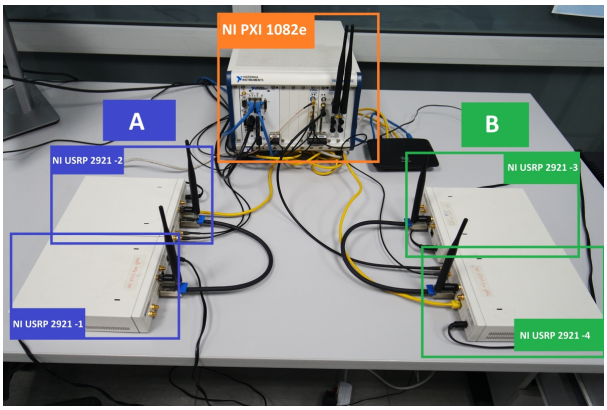

Figure 3: Measurement Setup

Table I: Testbed parameters.

Carrier Frequency	2.45 GHz
Transmit Gains	5-10 dB
Receiver Gains	0 dB
I/Q Data Rate	1 MS/sec
Number of Subcarriers (Fixed)	360
Zero Padding Length	120
FFT Length	480
CP Length	120
Total Number of Subcarriers in The Frame	600

The carrier frequency of system is chosen as 2.45 GHz. Quadrature Phase Shifting Key (QPSK) modulation is selected in tests and system parameters are shown in Table I. Zero forcing (ZF) equalization is used on the receiver.

One of the most common challenges is synchronization process of used USRP units applying SDR-based MIMO system. NI PXI-6683 module is used as the synchronization source in the tests. This module provides 10 MHz synchronization clock source from GPS module connected to the master clock. An external clock and a PPS signal are transmitted to first transmitter and receiver units over the cable. The second transmitter and receiver units, which are not connected with this cable, are synchronized by using MIMO cables. All symbols used as pilots; therefore, 4×360 dimensional channel coefficient matrices ($\mathbf{H}^{AB}$ and $\mathbf{H}^{BA}$) are obtained from each frame.

The obtained average amplitude and phase information of the channel coefficient vector pairs are observed as a result of tests. The obtained values for the amplitude and phase of the channel coefficient vectors have been calculated for 4 reciprocal channel pairs.

For quantization, we use one bit coding ($M = 1$) with 2 quantization levels in order to better demonstrate effects of L_1 and L_2 on error rates. For both directions, the tests are repeated 1000 times and the following results are obtained by averaging them. As described above, we measure KDR and KER values for different L_1 and L_2 sizes and different methods. Table II shows the KDR values for different methods and parameters. The maximum amplitude extraction method can be considered as the most successful with its low error rates. Furthermore it shows that phase information of the channel is not useful because of the high error rates.

Table III shows average KER values with different parameters. Values can be 1 or 0 for single comparison; therefore it simply indicates the match rate considering 1000 tests mentioned above. KER is useful to demonstrate quality of the general system. For larger subgroups, zero key error rate can be achievable. There is no value for channel phase based method in Table III,because all of KER measurements for this method were obtained to be 1.

After analyzing the effect of subgroup on error rates, we examine the effect of correlation between these subgroups. Under given L_1 and L_2 values, we change Δ_1 and Δ_2. In Figure 4, we can see the effect of frequency and space correlation between key elements. $\Delta_1/(\Delta_1 + L_1)$ is the frequency correlation ratio and $\Delta_2/(\Delta_2 + L_2)$ is the space correlation

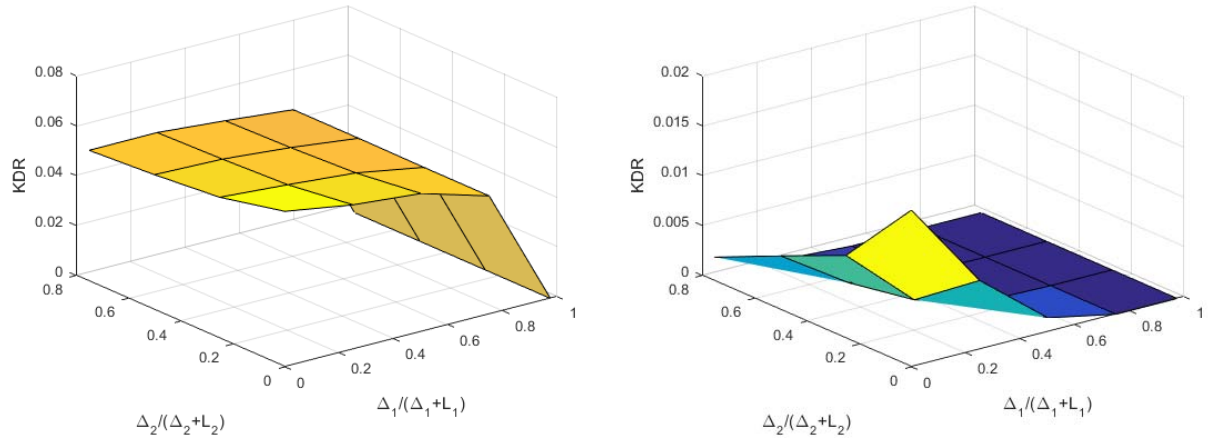

Figure 4: The effect of correlation in frequency and space on KDR. (a) Mean amplitude key extraction, (b) Maximum amplitude key extraction.

Table II: Key disagreement rates versus the key lengths considering amplitudes and phases of channel coefficients.

			Amplitude		Phase	
$g_{n',f'}$ (Subgrouping) by			Eq. 2 (Mean)	Eq. 4 (Max)	Eq. 2 (Mean)	Eq. 4 (Max)
L_2	L_1	Key Length (L)	KDR	KDR	KDR	KDR
1	1	1440	0.1004	0.1004	0.7360	0.7360
	12	120	0.0458	0.0025	0.7357	0.7633
	36	40	0.1063	0	0.7143	0.8
	60	24	0.0165	0	0.6898	0.8333
2	1	720	0.0735	0.0577	0.7361	0.7425
	12	60	0.0386	0.0003	0.7358	0.7671
	36	20	0.1049	0	0.7128	0.8001
	60	12	0.0150	0	0.6871	0.8333
4	1	360	0.0589	0.0356	0.7364	0.7474
	12	30	0.0329	0	0.7364	0.7474
	36	10	0.1021	0	0.7119	0.8001
	60	6	0.0147	0	0.6862	0.8333

Table III: Key error rates versus the key lengths considering amplitudes of channel coefficients.

			Amplitude	
$g_{n',f'}$ (Subgrouping) by			Eq. 2 (Mean)	Eq. 4 (Max)
L_2	L_1	Key Length (L)	KER	KER
1	1	1440	1	1
	12	120	0.895	0.23
	36	40	0.891	0
	60	24	0.109	0
2	1	720	1	1
	12	60	0.844	0.018
	36	20	0.879	0
	60	12	0.089	0
4	1	360	1	1
	12	30	0.593	0
	36	10	0.716	0
	60	6	0.076	0

ratio. Frequency correlation ratio is maximum 98% and space correlation is maximum 75% under 360 subcarrier and 2×2 MIMO with $L_1 = 6$ and $L_2 = 1$. We can see that, high levels of the correlation between following groups improve the key matching. The effect of frequency correlation rate is more effective than space correlation rate in terms of KDR. Furthermore, maximum amplitude key extraction method shows rapid decrease of KDR with increased correlation.

V. Conclusion

Four new PHY key extraction methods based on frequency and space grouping have been proposed and analyzed by the means of two different error measures through SDR tests. Maximum amplitude key extraction method has minimum KER and KDR values among the proposed methods.

References

[1] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp.

19–26, 2017.

[2] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[3] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[4] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1687–1700, 2013.

[5] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2578–2588, 2016.

[6] J. Choi and J. Ha, "Secret key transmission based on channel reciprocity for secure IoT," in *European Conference on Networks and Communications (EuCNC), 2016*. IEEE, 2016, pp. 388–392.

[7] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2016, pp. 1–5.

[8] S. Gopinath, R. Guillaume, P. Duplys, and A. Czylwik, "Reciprocity enhancement and decorrelation schemes for PHY-based key generation," in *GC Wkshps*. IEEE, 2014, pp. 1367–1372.

[9] S. Lv, X. Lu, Z. Lu, X. Wang, N. Wang, and L. Sun, "Zero reconciliation secret key extraction in MIMO backscatter wireless systems," in *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6.

[10] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in *ISSSE*, 2012, pp. 1–4.

[11] M. Guillaud, D. Slock, and R. Knopp, "A practical method for wireless channel reciprocity exploitation through relative calibration," in *Int. Symp. on Signal Processing and Its Applications*, vol. 1, August 2005, pp. 403–406.

[12] C. Chen, "Secret key establishment using wireless channels as common randomness in time-variant MIMO systems," 2010.

[13] *LabVIEW System Design Software*. [Online]. Available: http://www.ni.com/labview/