Rand-OFDM: A Secured Wireless Signal

Hesham Mohammed and Dola Saha
Department of Electrical & Computer Engineering
University at Albany, SUNY, Albany, NY 12222 USA
{hhussien, dsaha} @albany.edu

***Abstract*—Wireless communication has been a broadcast system since its inception, which violates security and privacy issues at the physical layer between the intended transmit and receive pairs. As we move towards advanced spectrum sharing methodologies involving billions of devices connected over wireless networks, it is essential to secure the wireless signal such that only the intended receiver can realize the properties of the signal. In this paper, we propose Rand-OFDM, a new waveform, secured with a shared secret key, where the signal properties can be recovered only at the expected receiver. We achieve the signal level security by modifying the OFDM signal in time-domain, thus erasing the OFDM properties and in turn obfuscating the signal properties to an eavesdropper. We introduce a key-based secured training signal for channel estimation, which can be used only at the intended receiver with prior knowledge of the key. As a final step for recovery of the signal, we use a clustering based technique to correct the phase of the received signal. Our cryptanalysis shows that Rand-OFDM is especially useful in future wide band signals. Extensive simulation and over-the-air experiments show that the performance of Rand-OFDM is comparable to legacy OFDM and SNR penalty due to the secured waveform varies between ≈ 1-4dB. In all these scenarios, Rand-OFDM remains unrecognized by the adversary even at the highest possible SNR.**

I. Introduction

As new spectrum (sub-6GHz, mmWave and TeraHertz) becomes available for communication and coexistence of frequency-agile cognitive heterogeneous nodes becomes a norm, we need to rethink physical layer security to provide maximum secrecy in a broadcast channel. There has been a growing interest recently among multiple federal agencies to utilize the spectrum in a collegial way by heterogeneous devices. This also indicates that wireless signals will be vulnerable to various security attacks, which was unforeseen in prior extremely regulated framework. This motivates us to investigate in physical layer secured communication, which is hard to decipher by an eavesdropper in a hostile scenario, as well as practical enough to be accepted for mass deployments.

Prior work [1]–[5] utilizes imperfection of the communication channel to establish secrecy by physical layer methods without the need of a shared secret key. However, channel imperfections are not enough to provide high secrecy capacity when the eavesdropper has a high signal-to-noise ratio (SNR) or has similar quantized channel state as the intended receiver. Higher layer encryption [6] provides computationally hard secrecy, but most of the last mile connection is a broadcast wireless channel, which is vulnerable to various security attacks. Since the waveform remains unchanged in all the above mentioned scenarios, it is plausible for the eavesdropper to restrict cryptanalysis search space within that waveform. To address these issues for future wireless agile radios, we introduce physical layer security, where we modify the OFDM waveform to completely disrupt its orthogonality properties of the subcarriers based on a shared secret key. At the receiver, we perform extensive channel estimation and reconstruct the waveform. The secret key can be derived from the channel or stored in the radio hardware, which will minimize the key distribution issues. In this paper, we only focus on modification of the time-domain signal at the transmitter and reconstruction of that back at the receiver.

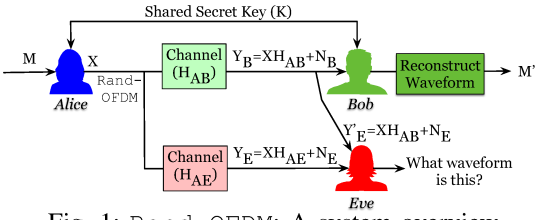


Fig. 1: Rand-OFDM: A system overview.

If M is the message that *Alice* needs to transmit to *Bob*, she can encrypt it with the shared secret key (K) to produce X. As it reaches *Bob*, it passes through the channel H_{AB}, such that the received signal is $Y_B = XH_{AB} + N_B$, where N_B is the noise. An eavesdropper, *Eve*, will experience a different channel and will receive $Y_E = XH_{AE} + N_E$. If channel imperfections are used to encrypt, secrecy capacity is a function of received SNR at *Eve*. In this scenario, we propose Rand-OFDM, where we modify the time domain signal, such that the transmitted signal, X, is no longer a known waveform (OFDM, CDMA, etc.). Figure 1 shows an overview of Rand-OFDM, where we randomize the time domain OFDM signal based on K, such that the resultant X does not have orthogonality property. Due to the spectral efficiency of OFDM and its use in most standards, like Wi-Fi [7], 5G [8], we have chosen it as the candidate for generating the base waveform.

Our approach has two distinct benefits over prior work. ***Firstly***, secret key based approach to modify the signal indicates that even at high SNR or even if *Eve* has full channel knowledge between *Alice* and *Bob*, H_{AB}, she will not be able to decode X. In other words, if *Eve* gets access to $Y'_E = XH_{AB} + N_B$, she will not be able to decode X without the key K, which is used to generate X. ***Secondly***, by modifying the time domain signal based on a key, we ensure that it appears as a noise or an unknown signal to *Eve*. The

combination of the key and data will create a different signal every time it is transmitted. Thus it creates a larger search space for *Eve* to attack this waveform. It is to be noted here that any higher layer encryption or bit level interleaving can be used in conjunction with `Rand-OFDM` to provide multiple layers of protection from different security threats.

The major challenges of `Rand-OFDM` are: 1) to design a computationally light operation to modify the OFDM waveform in time-domain, 2) to estimate the channel effects accurately at the receiver, which looses frequency domain properties due to the time domain modifications, 3) to hide the channel parameters in a way to make it difficult for the eavesdropper to estimate the channel accurately, and 4) to architect a design to correct the residual phase offsets due to the absence of pilot subcarriers in frequency domain. To the best of our knowledge, we are the first ones to *modify the time domain wireless OFDM signal to loose the orthogonality of the signal and introduce novel channel estimation technique to recover the signal back at the receiver and evaluated the system in practical over-the-air scenarios*. Hence, the key contributions of our work can be listed as follows:

Key-based Time Domain Security: We designed a secret key based time domain modification of the OFDM signal to generate a *new waveform*, `Rand-OFDM`, which does not retain any OFDM properties that are essential to combat the multi-path effects of the channel. At the receiver, we successfully reconstruct the signal by channel estimation and decryption of the `Rand-OFDM` waveform.

Secured Training Signal: We designed a novel training signal based on a shared phrase or data with the same randomization key, such that only the intended receiver is able to correctly decode it to estimate the channel accurately at the receiver.

Clustering based Phase Offset Correction: We scramble the signal in time domain, where the frequency domain pilots change in both phase and magnitude and cannot be used as known symbols for channel estimation or phase tracking. We introduced a *unique* solution to track the residual phase offset by utilizing K-medoids clustering algorithm underneath.

Cryptanalysis: We perform cryptographic analysis on the `Rand-OFDM` signal, and provide insights on the resiliency of the waveform, specially for higher orders of FFT, as envisioned in next generation of wireless systems.

Practical Evaluation: In midst of mostly theoretical research in time domain physical layer security, we formulated the mathematical problem for `Rand-OFDM` and provided a receiver design that is essential for successfully decoding the signal in multipath-rich environment. We also evaluated our system using extensive experiments over the air in an indoor environment for the protocol to be embraced for practical deployment.

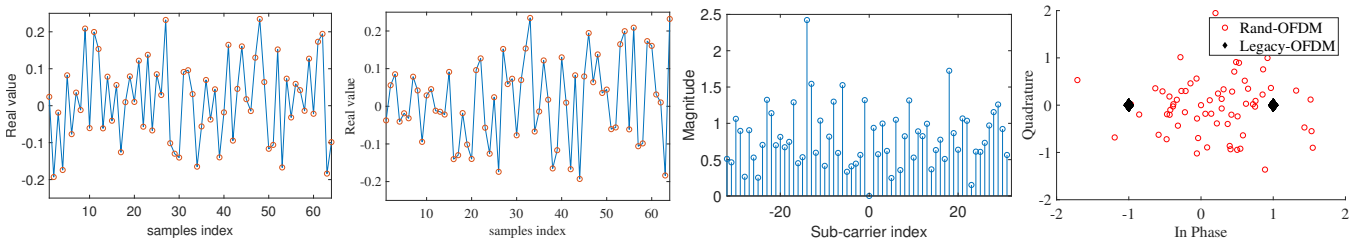
II. Related Work

Time domain security: A fairly decent amount of research has been done in recent years to modify the time domain signal to achieve security in physical layer. However, most of them are either theoretical or are dependent on impractical assumptions. In [9], authors introduced an OFDM encryption scheme based on multiplying the real and the imaginary parts of the generated OFDM by dynamic values based on a shared secret key between the transmitter and the receiver. This changes the signal values, which changes the Peak-to-Average Power Ratio (PAPR) of the OFDM symbol. The results are evaluated only for simulated AWGN channel, where there is no channel effects. Authors in [10] uses a random shuffling based on a secret key. The algorithm has been evaluated for a flat fading channel, where channel effects are negligible. These works do not attempt to introduce any channel or phase correction at the receiver due to theoretical nature of these research.

In [11], authors propose a time domain physical layer security scheme based on modifying the length of the cyclic prefix (CP) to be equal to the channel impulse response of the intended user, whereas the channel impulse of *Eve* may be longer than the intended user. This introduces inter symbol interference (ISI) to the received signal of the Eve. However, if *Eve* has a better channel compared to *Bob*, this technique fails. In [12], authors propose adding an artificial noise to the time domain OFDM signal such that when it passes through the receiver channel, it gets accumulated on the Cyclic Prefix. The receiver can decode the message after removing the CP, while the eavesdropper's signal can not be recovered due to the presence of the noise. This is also a theoretical attempt without any receiver modification in practical scenarios.

Frequency domain secrecy: Modifying the frequency domain signal is a common technique to achieve secured [13]–[16] or covert communication [17]. In [13], the transmitter uses the non fading subcarriers to the intended user for data transmission. The assumption of this theoretical work is that *Eve*'s channel has a completely different deep fading, which might not be a practical assumption. In [14], the authors proposed an algorithm to provide pre-coder and post-coder matrices to make the channel matrix of the legitimate user to be diagonal. Also the authors in [15] proposed an optimal channel selection for channel indices to maximize the SINR for the legitimate user to achieve secure communication. In [16], the author proposed an encryption algorithm for OFDM system based on dummy data insertion of a portion of sub carrier to make performance degradation at the eavesdropper. It is to be noted that frequency domain modification retains the OFDM properties and reveals the waveform characteristics to the eavesdropper.

Space domain secrecy: Use of MIMO antennas [18]–[20] to beamform towards the intended receiver and/or steer null towards the eavesdropper is another way to enable physical layer security. The two major assumptions in these set of work are a) *Eve* will have fewer antenna elements, which cannot be accurate in the world of electronic warfare and b) *Eve* is not in the path of beam pattern radiation, which is inaccurate specially when devices are getting smaller and can be placed anywhere in plain sight.



(a) Time domain OFDM signal before randomization (b) Time domain `Rand-OFDM` signal after randomization (c) Frequency response of `Rand-OFDM` signal (d) Constellation diagram of BPSK-modulated `Rand-OFDM`.

Fig. 2: Time domain and frequency domain representation of `Rand-OFDM` at the transmitter.

III. Background

Orthogonal Frequency Division Multiplexing (OFDM) is a digital multicarrier modulation technique, where subcarriers are orthogonal to each other. This is achieved by Inverse Fast Fourier transform (IFFT) on the modulated data stream. For N parallel data streams, $N - point$ IFFT is performed on the complex digital modulated signal $X(n)$. The time domain signal $x(n)$, can be expressed as:

$$x[n] = IFFT(X[n]) = \sum_{i=1}^{N-1} X(i) e^{\frac{j2\pi in}{N}} \tag{1}$$

In order for the IFFT/FFT to create an intersymbol interference (ISI) free channel, the channel must appear to provide a circular convolution. Hence, a cyclic prefix of length v is appended after the IFFT operation, resulting in N + v samples, which are then sent in serial through the wireless channel.

The duality between circular convolution in the time domain and simple multiplication in the frequency domain is a property unique to the Discrete Fourier Transform (DFT), which can be utilized to represent the received OFDM signal $Y(n) = H(n)X(n)$.

At the receiver, the cyclic prefix is discarded, and the N received symbols are demodulated, using an FFT operation, which results in N data symbols. The received frequency domain signal $Y(n)$ is given by:

$$Y[n] = FFT[y(n)] = \sum_{i=1}^{N-1} y(i) e^{\frac{-j2\pi in}{N}} \tag{2}$$

where y is the received OFDM symbol in the time domain.

IV. System Design of `Rand-OFDM`

In this section, we introduce the system design of `Rand-OFDM`, which predominantly has modifications at both the transmitter and the receiver side. The key idea of `Rand-OFDM` lies in randomizing the FFT output or the time domain digital complex signals to loose the OFDM properties, such that it appears as a wideband noise to the eavesdropper. Figure 2 shows such an example a) time domain signal after the IFFT output, followed by b) its randomized version, which is transmitted over the air. The c) frequency response of the transmitted `Rand-OFDM` signal and d) its constellation plot show that we have successfully destroyed the OFDM properties for the signal to appear as a noise at the transmitter side, even before the channel impairments are introduced. Figure 3 shows the transmitter and receiver modules, which are discussed in § IV-A and § IV-B respectively.

A. *Transmitter Design of* `Rand-OFDM`

`Rand-OFDM` transmitter is based on Wi-Fi [7] like OFDM [21] building blocks. We introduce a new block termed *Randomizer* after the IFFT block in the OFDM transmitter chain, as shown in figure 3. The *Randomizer* introduces time domain scrambling of the resultant time domain complex samples from the IFFT block. The time domain scrambling is based on a shared secret key between the transmitter and the receiver pair. In other words, this is the symmetric key that is used both in encryption and decryption process. For example, if the original OFDM symbol is $[a_0, a_1, a_2, a_3, a_4, a_5]$, then the resulted randomized sequence is $[a_5, a_3, a_1, a_2, a_4]$, where the key is $[5, 3, 1, 2, 4]$. The cyclic prefix (CP) is added after that to be able to extract frequency response of the channel at the receiver, which is detailed in § IV-B.

As the *Randomizer* block is added in the OFDM transmitter chain, the time domain `Rand-OFDM` signal, x_t, can be expressed as:

$$x_t = P_{CP} R F^{-1} X_F \tag{3}$$

where P_{CP} is the cyclic prefix matrix, R is the randomizer matrix and F^{-1} is the inverse Fourier Transform Matrix.

By randomizing in time domain, the secured transmitted wave form has lost all the OFDM properties. In other words, the `Rand-OFDM` transmitted wave form X_t can given by:

$$X_t = F T x_t = F R F^{-1} X_F \tag{4}$$

where T is the truncation matrix for cyclic prefix removal and F is the N-FFT matrix and can be given as:

$$F = \begin{bmatrix} W^{0,0} & W^{0,1} & ..... & W^{0,N-1} \\ W^{1,0} & W^{1,1} & ..... & W^{1,N-1} \\ . & & & \\ . & & & \\ W^{N-1,0} & W^{N-1,1} & ..... & W^{N-1,N-1} \end{bmatrix} \tag{5}$$

where $W^{n,k} = e^{-2j\pi \frac{nk}{N}}$ and N is the FFT size.

$$FRF^{-1} = \frac{1}{N} \sum e^{2j\pi \frac{n(k-m)}{N}} = \begin{cases} I, & R = I \\ Q, & R \neq I \end{cases} \tag{6}$$

where I is the identity matrix and Q is the generated transformation matrix due to the presence of R.

From equation 6, we can conclude that if there is no randomization in the time domain samples (i.e $R_F = I$), the OFDM symbol retains its orthogonality property. Otherwise,

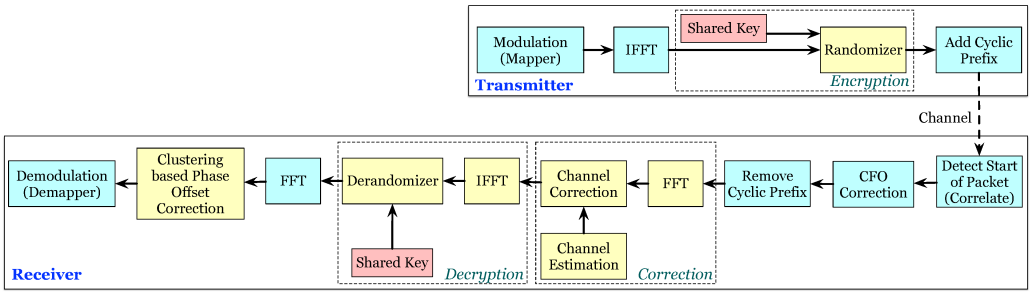


Fig. 3: Transmitter and receiver blocks in Rand-OFDM. Blocks in yellow are either added or modified in the legacy system.

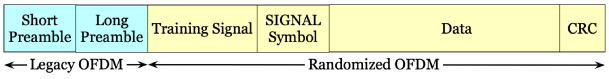


Fig. 4: Packet Structure of Rand-OFDM.

a magnitude and phase noise is added to the received OFDM symbol. This distorts the original OFDM symbol by transforming the original constellation into a random constellation pattern which depends on the randomization matrix R. We would like to highlight here that the changes introduced in this stage do not depend on the original modulation order of the transmitted constellation. Moreover, the transformation matrix spreads the power of the OFDM symbol over the whole bandwidth including the guard bands. Figure 2 shows the transformation of an OFDM symbol to a Rand-OFDM symbol. In this case, 52 subcarriers were modulated with BPSK modulated signal, generating the time domain OFDM signal as in figure 2a. The resultant signal goes through a *Randomizer* to generate the Rand-OFDM waveform as shown in figure 2b. If we perform FFT on this waveform, we notice that the magnitude of the subcarriers are varying randomly, as well as the power spreads to all 64 subcarriers and not confined to only 52, as we started with. This is evident in figure 2c, which is due to the matrix multiplication of R. Figure 2d shows the phase noise that is induced due to the randomization. These imperfections require significant modifications in the receiver design, which is explained in § IV-B.

The packet structure of Rand-OFDM is shown in figure 4, where the short and long preambles of legacy 802.11 [7] system are used to detect the start of the packet. Rest of the MAC layer packet structure remains same except they are modified just before transmission to the Rand-OFDM waveform. A training signal of one OFDM symbol duration is appended to improve the channel estimation at the intended receiver, the design of which is detailed in § V-A.

B. Receiver Design of Rand-OFDM

The receiver design of Rand-OFDM is based on legacy 802.11a/g [7] receiver blocks, where yellow colored blocks are the ones which we added or modified, as shown in figure 3. Receiver design starts with a packet detection block, followed by Carrier Frequency Offset (CFO) correction and removal of cyclic prefix. FFT follows right after that to convert the data to the frequency domain. Based on the modifications at the transmitter, it might seem that we need to insert the *Derandomizer* block just before the data goes into the FFT block. One of the major components before the FFT is the channel correction, as the received waveform can be represented as:

$$Y_t = H_t X_t + N_t = H_t P_{CP} R F^{-1} X_F + N_t \quad (7)$$

where H_t is the channel impulse response in time domain and N_t is the noise. At this point, we need to estimate and correct the channel impairments at the receiver. Time domain channel estimation and correction has been shown to be computationally more expensive [22], due to which we choose to perform it in frequency domain. Derandomizing the signal before extracting the channel information would make the channel estimation problem intractable. Hence, we convert the signal to frequency domain to extract the frequency domain channel response, which is first corrected on the signal. Once the cyclic prefix is removed, we perform N-point FFT to convert the time domain signal Y_t to frequency domain. The received waveform in frequency domain can then be expressed as:

$$X_{rF} = FTY_t = H_F F R F^{-1} X_F + N_F \quad (8)$$

where H_F is the channel frequency response. Channel estimation for Rand-OFDM is discussed in details in § V-A. In the following discussion, we assume that we know the channel H_F and inverse it yielding received frequency domain waveform $\tilde{X}_{rF}$ without channel impairments.

$$\tilde{X}_{rF} = H_F^{-1} X_{rF} = F R F^{-1} X_F + \tilde{N}_F \quad (9)$$

This is the output of the channel correction block as shown in figure 3, which is in frequency domain. We introduced the randomization in time domain, and hence it is necessary to convert it back to time domain as a part of the decryption block. After the signal is passed through the IFFT block of the decryption process, it can be represented as

$$F^{-1}\tilde{X}_{rF} = F^{-1} F R F^{-1} X_F + \tilde{N}_F = R F^{-1} X_F + \tilde{N}_F \quad (10)$$

Now, this time domain signal is passed through the *Derandomization* block to yield the correct time domain data symbols.

$$R^{-1} R F^{-1} X_F + \tilde{N}_F = F^{-1} X_F + \tilde{N}_F \quad (11)$$

The final step is to perform FFT on equation 11 to demodulate the data subcarriers.

$$F F^{-1} X_F + \tilde{N}_F = X_F + \tilde{N}_F \quad (12)$$

We introduce another Phase Offset Correction phase, which is detailed in § V-B.

V. Distortions from Channel and Hardware

Imperfections at the received are induced due to the wireless multipath channel and the underlying hardware. In this section, we illustrate the methodologies that we introduce to estimate and counteract the imperfections to yield better performance.

A. Training signal based channel estimation

Accurate estimation of channel is essential in high frequency selective fading channels, specially at higher order modulations, where minimal error in channel estimation will lead to significant error in demodulation. In § IV-B, we assumed complete knowledge of the channel H_F, which is an incorrect assumption in practical systems. Partial channel estimation on only 52 subcarriers of long preamble and extrapolating that for 64 subcarriers, as required for `Rand-OFDM`, yields poor performance in multipath channels. Hence, we design a training signal that spans all 64 subcarriers to better estimate the channel at the intended receiver. We use a shared secret data and randomize it based on the same shared key between *Alice* and *Bob* to create one BPSK modulated `Rand-OFDM` signal, as described in § IV-A. This OFDM symbol is transmitted after the preamble as shown in figure 4. Channel estimation at the receiver requires knowledge of transmitted waveform, which in this case is secured by the shared key. Hence, we add another layer of security, where Eve will not be able to estimate the channel accurately as the training signal is dependent on the shared secret key, and physical layer authentication can be initiated using the training signal [23], [24].

If X_{Tr} is the BPSK-modulated OFDM signal, then the `Rand-OFDM` training signal can be derived from equation 3 as $x_{Tr} = P_{CP}RF^{-1}X_{Tr}$. The received training signal can be derived from equation 7 as

$$y_{Tr} = H_t P_{CP} R F^{-1} X_{Tr} + N_{Tr} \tag{13}$$

Since X_{Tr} and R matrices are shared between the transmitter and the intended receiver only, the channel can be estimated by only *Bob*. Ignoring the noise, channel frequency response can be estimated by:

$$H_F = \frac{FTy_{Tr}}{X_{Tr}} \tag{14}$$

Figure 5 shows the actual and the estimated phase and magnitude of the channel in frequency selective fading conditions. It is obvious that training signal channel estimation gives an accurate channel estimation for the whole 64 sub-carriers rather than the preamble channel estimation which only concerns on 52 sub-carriers .

B. Clustering based phase offset correction

Device impairments introduce difference between the carrier frequency of the receiver and that of the transmitter. Coarse and fine carrier frequency offset correction blocks are introduced at the receiver to estimate and correct those offsets based on short and long preambles respectively, as shown in figure 3. Residual carrier frequency offset of conventional OFDM received waveform is calculated based on the pilot subcarriers. In `Rand-OFDM`, the pilots inserted in frequency domain do not capture the channel frequency response at those subcarriers as the pilot energy gets spread due to the process of randomization. Hence, we introduce a clustering based algorithm to track the residual phase offset due to hardware impairments. It is to be noted here that the purpose of this block is not to estimate the variation in channel per OFDM symbol, which can be accurately estimated by inserting pilot subcarriers in every OFDM symbol. This block is intended to estimate and correct the offset between the transmitter and receiver pairs, which do not change from one OFDM symbol to the next.

We use K-mediods clustering algorithm [25], where the input to the algorithm is the In-Phase and Quadrature values of the constellation points of all the subcarriers of all received OFDM symbols in a packet and the number of expected clusters based on the modulation order. The resultant C cluster centers are then examined to estimate the residual phase offset. We choose the farthest cluster points in each quadrant to determine the phase offset. There are also the highest energy point indicating a total of 4 cluster centers for QAM or QPSK modulations and only 2 for BPSK. The rationale for choosing the highest energy point within a quadrant is that there exists only one such point in the transmitted constellation to which it can be mapped to. This is a generic approach and can be scaled to even higher order modulations, like 256-QAM and beyond. The phase offset is then calculated per quadrant as:

$$\theta_{estimated,i} = arg(X_{Ti}/C_{max,i}) \tag{15}$$

where X_{Ti} is the farthest transmitted constellation point within a quadrant and $C_{max,i}$ is the maximum energy cluster center of the same quadrant i. Averaging 2 values in BPSK or 4 for other modulation orders, we calculate residual phase offset as:

$$\theta_{estimated} = \frac{1}{M}\sum_{i=1}^{M}\theta_{estimated,i} \tag{16}$$

where M is 2 for BPSK and 4 for other modulations. In the last step, we correct the residual phase offset by multiplying the estimated phase to the received signal to generated the corrected signal, X_{Fc}, which can then be used for demodulation.

$$X_{Fc} = X_F e^{j\theta_{estimated}} \tag{17}$$

where X_F is the received OFDM signal before correction. Figure 6 shows an example scenario of over-the-air experiments at 15dB SNR, where the residual phase offset is corrected based on the proposed clustering algorithm.

VI. Cryptanalysis

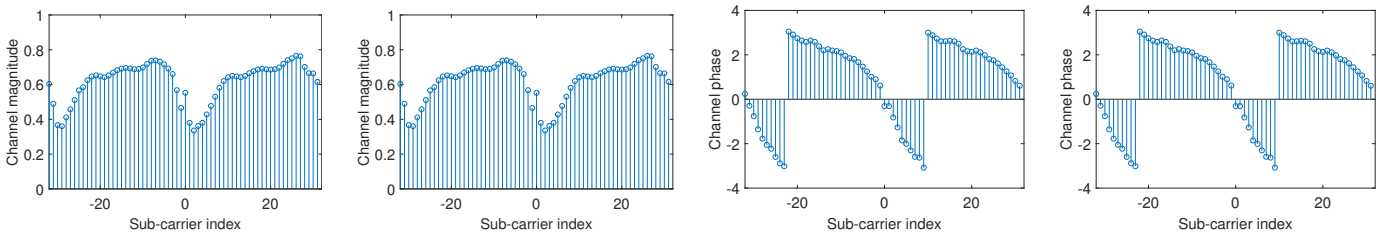
In this section, we perform security analysis on `Rand-OFDM` to evaluate its resiliency against various types of attacks. For simplicity, let's assume that the received OFDM symbol at *Eve* is:

$$Y_E = FRF^{-1}X_F \tag{18}$$

According to Shannon secrecy [26], the system can be perfectly secure if the key size equals to the data size such that:

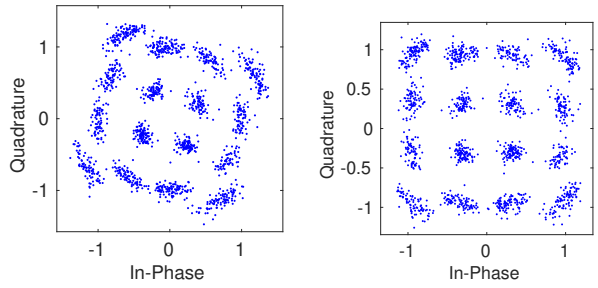
$$E(R_i) \geq E(X_F) \tag{19}$$

where $E(X)$ is the entropy of the random variable X. This analysis can easily be realized in bit level, however in physical layer we observe it from two different viewpoints. *First*, the system achieves perfect secrecy on symbol level



(a) Actual Channel (Mag) (b) Estimated Channel (Mag) (c) Actual Channel (Ph) (d) Estimated Channel (Ph)

Fig. 5: Channel Estimation (Magnitude & Phase) of frequency selective channel for training signal based estimation technique.



(a) Before Phase correction (b) After Phase correction

Fig. 6: Clustering based residual phase offset correction for over the air indoor experiments using 16QAM modulation.

as both the data symbol size and the key size are equal to the FFT size N. In other words, *Eve* can not deduce any information with one symbol. *Second*, if the system has a set of keys $K = [K_1, K_2, K_3, ..., K_V]$, and OFDM frame $X = [X_1, X_2, X_3, ..., X_n]$, the mutual information between the encrypted and original symbols equal to:

$$\lim_{V \to n} I(X_E, X_F) = 0 \tag{20}$$

A. Brute-force attack

In this attack, the eavesdropper knows the encryption and the decryption algorithm, however the key is unknown. The eavesdropper performs an exhaustive search on all possible keys to decrypt the cipher data (i.e the encrypted data). The strength of the algorithm is proportional to the length of the key, which is the size of FFT for `Rand-OFDM`. The number of all possible keys L is given by $L = N!$, where N is the FFT size. So the probability of success P_s to predict the key is uniformly distributed and is given by $P_s = \frac{1}{L}$. FFT size has been chosen to be 64, which is minimum for 802.11a/g [7], and can be a much larger value of 1024 or 2048 in newer wideband Wi-Fi and 5G standards.

B. Cipher text attack

In this attack, Y_E is only available with the decryption function D. *Eve* tries to predict R_E by attempting different keys based on the statistical properties on the cipher data. However, since the security layer is introduced in physical layer, especially in time domain, the statistical properties of the received waveform does not change, for example received power or the peak to average power ration (PAPR). So *Eve* has to try all possible keys to decrypt the data, resulting in Brute-force attack.

Channel	AWGN	Flat	Frequency Selective
Model	-	Rayleigh	Rayleigh
No. of taps	0	1	6
Path delays	0	0	[0,100,200,300,500,700] ns
Path loss	0	0	[0,-3.6,-7.2,-10.8,-18,-25.2] dB
Doppler	0	0	3Hz

TABLE I: Channel Models

C. Chosen plain text attack

In this attack, Y_E and X_F are known at the eavesdropper. In other words, *Eve* knows some pattern and the corresponding cipher patterns. For fixed key, *Eve* can solve equation 18 and deduce the corresponding R_E. However the security of the algorithm can be increased by using a defined shared set of keys $K = [K_1, K_2, ..., K_V]$, and the selected shared key changed dynamically from one symbol to another based on certain distribution $f_K(K)$. In this case, *Eve* has to deduce the statistical properties of the key distribution for multiple attacks assuming K is known.

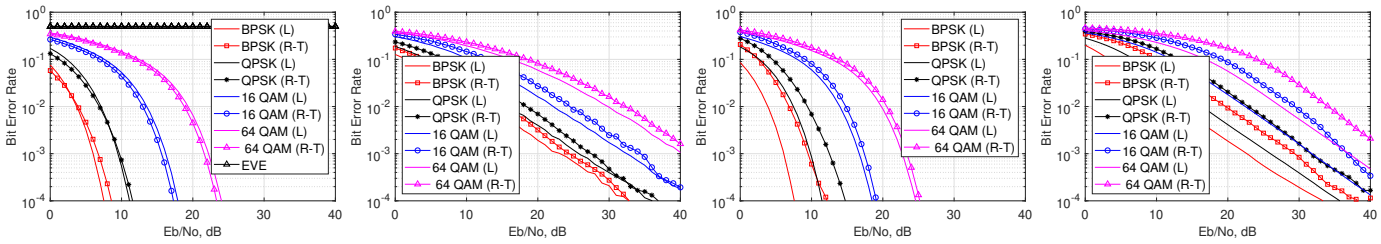
VII. Evaluation

In this section, we present the performance analysis of the `Rand-OFDM` system in comparison with legacy 802.11a/g in different channel models. Although we do not use any pilot symbols, they are still inserted as in the legacy system such that same number of data bits are transmitted for both the cases. We used MATLAB to encrypt and decrypt the signals and used the channel models to perform extensive simulations for both legacy OFDM and `Rand-OFDM`. For the rest of the paper, the suffixes (L) and (R) are used for legacy OFDM [7] and `Rand-OFDM` transmissions with full channel knowledge respectively. In addition, we use (R-T) using training signal based channel estimation.

A. Without Channel Estimation

We evaluate the performance of `Rand-OFDM` receiver blocks as described in § IV-B in the basic scenario, where no channel estimation is required.

1) AWGN Channel: The first case for evaluation is Additive White Gaussian Noise (AWGN) channel, where the channel frequency response matrix $H_F = I$, since both time and frequency coefficients are unity. Figure 7a shows the BER performance of `Rand-OFDM` in AWGN channel for different modulation orders. Performance of `Rand-OFDM` is close to that of legacy OFDM signal. This is due to the fact that OFDM structure, even when lost, can be reconstructed back at the receiver in the absence of channel effects. From equation 10,



(a) AWGN Channel. (b) Indoor channel. (c) Flat fading channel. (d) Indoor channel.

Fig. 7: BER of `Rand-OFDM` compared to legacy OFDM. Figures (a,b) with complete channel knowledge and (c,d) with training signal channel estimation.

it is evident that if the eavesdropper does not have the key to generate the matrix R, she can not decode the packet. This is shown in the results as well, where the BER curve for *Eve* remains constant and never go down even at higher SNRs. This is a major advantage of using key-based physical layer security over channel based encryption techniques. We choose not to show the BER curve for *Eve* as she was unable to decode in the best possible channel.

2) Complete channel knowledge: In this section, the performance of the proposed system is evaluated assuming that we have full channel knowledge (i.e H_F is known). Based on ITU-R recommendation, we assume frequency selective indoor channel model with parameters shown in table I. We assume that legacy receiver also knows the H_F matrix. Figure 7b shows the performance of `Rand-OFDM` in a frequency selective channel when the channel is known at the receiver. If channel is known, the SNR gap between legacy OFDM and `Rand-OFDM` is due to the modification of the waveform, which cannot be retrieved at the receiver.

B. With Channel Estimation

In this section, we analyze the performance of the channel estimation techniques, as elaborated in § V-A in two different channel models, 'Flat Fading' and 'Frequency Selective Fading', as shown in table I.

Training signal is used to estimate the wireless channel effect for `Rand-OFDM` transmissions, while legacy OFDM signal did not require this extra OFDM symbol. Figure 7c shows the performance of the training signal based channel estimation, which performs well due to the accuracy of the channel estimation using the training signal channel estimation. there is a small SNR penalty around $\approx 2dB$ due to the loss of orthogonality due to the randomization process at the transmitter. This is expected as the channel effects are minor in a relative flat channel. Figure 7d shows the performance in a multipath rich environment, where the channel is extremely frequency selective. Results indicate that the newly introduced training signal is not only secured, but also provides accurate channel estimation for the signal to be reconstructed back with minimal SNR penalty. The SNR gap between legacy OFDM and `Rand-OFDM` is $\approx 4dB$, indicating that it can be embraced in various practical scenarios.

VIII. Over the Air Experiments

We perform extensive over-the-air experiments in indoor scenario to validate `Rand-OFDM`. Figure 9 shows one of our transceiver nodes equipped with USRP X310 [27] with 10 dBi antenna. It is connected to an Intel NUC (NUC7i7BNH) with i7-7567U processor and 16GB DDR4 memory for faster processing of the I/O. The experiments are performed in multiple locations in a multipath-rich indoor environment in both line of sight and non-line-of-sight scenarios. We present the results for an average of all those locations to eliminate any dependencies on channel. Also, all the experiments were performed at 20MHz bandwidth and 2.484GHz frequency to avoid any interference from the Wi-Fi Access Points operating in the same area. Each data point in our result is an average of 500 OFDM symbols for both legacy OFDM and `Rand-OFDM`.

Figure 8 shows the BER performance for legacy and `Rand-OFDM` transmissions for different modulation orders. It is evident that there is an SNR gap between the `Rand-OFDM` and the Legacy OFDM transmission. This gap is due to the loss of orthogonal property of OFDM signal and channel estimation imperfections. This is the SNR penalty that we incur to secure a waveform in time domain. Moreover, the SNR gap decreases at higher modulation order due to the higher operated SNR, which enables the receiver to decrease the error space in channel estimation using the training signal. In other words, the error introduced due to time-domain modification can be reconstructed back more efficiently at a higher SNR.

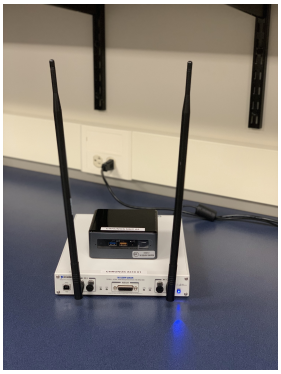
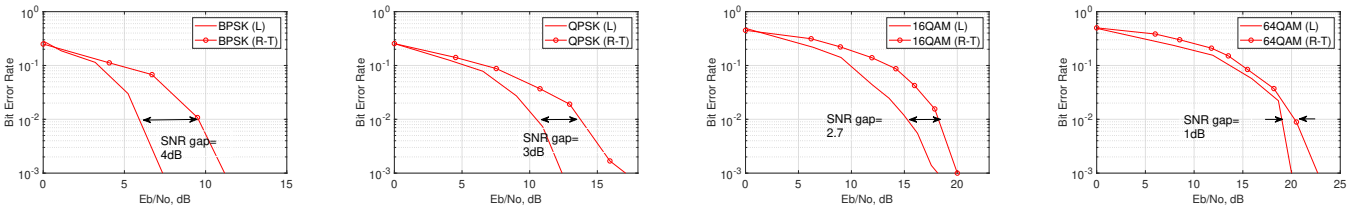


Fig. 9: Experimental setup of one node.

Figure 10 presents the phase angle correction distribution for different modulation orders over all packets at different SNRs. The residual phase error is dependent on the hardware impairments and not on modulation order or channel characteristics. This is evident from the values, which varies between 0.05 to 0.12 radians. The phase correction results indicate that there exists significant residual error, which needs to be corrected to improve the performance.



(a) BPSK (b) QPSK (c) 16QAM (d) 64QAM

Fig. 8: BER of `Rand-OFDM` compared with legacy OFDM for over-the-air experiments using different modulation orders.

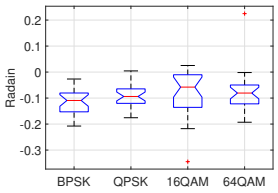


Fig. 10: Residual phase offset correction for different modulation orders.

IX. Conclusion

In this work, we present `Rand-OFDM`, a secure OFDM transmission based on time domain scrambling using a shared secret key between the transmitter and the receiver. We perform channel estimation and equalization to retrieve the signal. Furthermore, we introduce a secured training signal to accurately estimate the channel followed by cluster based residual phase error correction. Over the air experiments show the success probability of this system. In future, the key generation and management can be developed based on channel state for lightweight secured physical layer encryption.

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. [Online]. Available: https://www.pnas.org/content/114/1/19

[2] J. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. PP, pp. 1–1, 10 2018.

[3] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys Tutorials*, vol. 14, no. 2, pp. 355–379, Second 2012.

[4] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 428–445, First 2013.

[5] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, Secondquarter 2015.

[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[7] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society : LAN/MAN Standards Committee. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[8] S. Sesia, I. Toufik, and M. Baker, *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Wiley Publishing, 2009.

[9] F. Huo and G. Gong, "A new efficient physical layer ofdm encryption scheme," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 1024–1032.

[10] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "An efficient ofdm-based encryption scheme using a dynamic key approach," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 361–378, 2018.

[11] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of ofdm systems using channel shortening," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–5.

[12] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap ofdm with discrete inputs," *Wireless Communications, IEEE Transactions on*, vol. 12, 02 2013.

[13] E. Güvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Communications Workshops (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 813–818.

[14] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for ofdm systems along with hardware implementation," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017, pp. 1338–1343.

[15] J. M. Hamamreh, E. Basar, and H. Arslan, "Ofdm-subcarrier index selection for enhancing security and reliability of 5g urllc services," *IEEE Access*, vol. 5, pp. 25 863–25 875, 2017.

[16] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an ofdm physical layer encryption scheme," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2114–2127, 2016.

[17] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *Information Hiding*, M. Kirchner and D. Ghosal, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 160–175.

[18] S. Shafiee and S. Ulukus, "Achievable rates in gaussian miso channels with secrecy constraints." in *ISIT*, 2007, pp. 2466–2470.

[19] Z. Rezki and M.-S. Alouini, "On the finite-snr diversity-multiplexing tradeoff of zero-forcing transmit scheme under secrecy constraint," in *2011 IEEE International Conference on Communications Workshops (ICC)*. IEEE, 2011, pp. 1–5.

[20] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect csi," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2010.

[21] S. Weinstein and P. Ebert, "Data transmission by frequency-division multiplexing using the discrete fourier transform," *IEEE transactions on Communication Technology*, vol. 19, no. 5, pp. 628–634, 1971.

[22] C. Suh, C.-S. Hwang, and H. Choi, "Comparative study of time-domain and frequency-domain channel estimation in mimo-ofdm systems," in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, vol. 2. IEEE, 2003, pp. 1095–1099.

[23] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *2007 IEEE International Conference on Communications*. IEEE, 2007, pp. 4646–4651.

[24] ——, "Using the physical layer for wireless authentication in time-variant channels," *arXiv preprint arXiv:0907.4919*, 2009.

[25] L. Kaufman and P. Rousseeuw, *Clustering by Means of Medoids*, ser. Delft University of Technology : reports of the Faculty of Technical Mathematics and Informatics. Faculty of Mathematics and Informatics, 1987. [Online]. Available: https://books.google.com/books?id=HK-4GwAACAAJ

[26] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[27] Ettus, *X310*, available at https://files.ettus.com/manual/page_usrp_x3x0.html.