A Novel Physical Layer Authentication with PAPR Reduction based on Channel and Hardware Frequency Responses

Prasidh Ramabadran, *Student Member, IEEE,* Pavel Afanasyev, David Malone, *Member, IEEE,* Miriam Leeser, *Senior Member, IEEE,* Darragh McCarthy, Bill O'Brien, *Member, IEEE,* Ronan Farrell, *Member, IEEE,* John Dooley, *Member, IEEE,*

***Abstract*—Next generation wireless communications such as 5G are expected to feature wide channel bandwidths on the order of hundreds of MHz. As bandwidths increase, circuit impairments caused by frequency dependent behaviour such as ripple and tilt in gain and group delay become more significant. PAPR of OFDM signals also increase with increasing number of sub-carriers. Transmitter circuit characterisation for the wide-band frequency response is needed to pre-compensate the signal to be transmitted. In this paper, we propose a novel scheme which uses the circuit characteristics combined with the channel response to generate the keys for encrypting signals to provide an additional tier of security at the physical layer. The modulated constellation of the signal of interest is encrypted by dispersing its phases in addition to encrypting the bits using Diffie Hellmann scheme. It is also shown that the method is able to reduce the PAPR of OFDM signals. This scheme is experimentally validated from end-to-end on a millimetre wave wireless link at 28.9 GHz demonstrating security against a well-positioned eavesdropper and a reduction of PAPR by 3.5 dB in a 2048 point OFDM signal with 1664 active QPSK modulated sub-carriers.**

***Index Terms*—Encryption; Wireless Communication; Physical Layer Security; Peak to Average Power Ratio.**

I. Introduction

MODERN wireless communications involve transmission of digital data over vector modulated radio frequency (RF) carriers. Unlike, wired communication schemes, wireless data transmission is of broadcast nature where the occurrence of transmission is sensed and can be received by multiple receivers including the legitimate nodes and eavesdroppers. The security of the data transmitted depends on the ability to encrypt the data such that only the legitimate receivers are able to interpret the message. This task is conventionally handled in the higher layers of the network protocol stack with techniques such as scrambling, bit and packet encryption. These techniques however do not encrypt the air interface of the wireless network and therefore leave the nodes open for traffic analysis and interception by eavesdroppers and man-in-the-middle platforms [1], [2]. One of the ways to reduce the probability of interception by an unauthorized node is to provide a degree of security in the physical layer (PHY) independent of the network protocols and infrastructure. Physical layer security has been gaining interest among researchers in recent years. A number of PHY security schemes such as data encryption in physical layer [1], [3]–[9], directional modulation [10], RF fingerprinting, and discrete Fourier transform spread orthogonal frequency division multiplexing (DFT-S-OFDM) have been proposed [10]–[14].

Data encryption in the physical layer involves scrambling the bit stream with a secret code that is mutually agreed by the legitimate nodes and unknown to eavesdroppers. In [1], the genuine nodes operate in a timed manner. The two nodes exchange packets of data sequentially at 2.4 GHz (802.11 standard) where the receivers run a level crossing algorithm to parse the received bits. The time indices where valid bits were found are recorded at both nodes and exchanged after a sufficient number of probes. An eavesdropper would get information on the time indices but not the parsed values thereby maintaining secrecy between the genuine nodes. In [3], [4], the key is generated from the channel variation statistics instead of using the current channel state information to generate the encryption keys. In [3], the proposed scheme is experimentally validated using software defined radio (SDR) modules configured for operation in accordance with the WiFi standard. In [7], the authors exploit the channel reciprocity between two legitimate nodes in a given time-slot to probe the channel with preamble of the 802.11i standard to generate symmetrical encryption keys at the two nodes which are used to scramble the data before transmission. A similar scheme employing discrete Fourier transform spread orthogonal frequency division multiplexing (DFT-S-OFDM) has been proposed in [10]. In all these schemes, the probing signal chosen is OFDM modulated. This provides a very convenient stimulus where the amplitudes and phases of sub-carriers are well defined but exhibits a high PAPR (Peak to Average Power Ratio). PAPR of a complex envelope modulated signal s(t) may

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant Number 13/RC/2077 Prasidh Ramabadran, David Malone, Pavel Afanasyev, Darragh McCarthy, Ronan Farrell and John Dooley are with National University of Ireland, Maynooth, Co. Kildare, Republic of Ireland (e-mails:prasidh.ramabadran@mu.ie, david.malone@mu.ie pavel.afanasyev.2017@mumail.ie, darragh.mccarthy@mu.ie, john.dooley@mu.ie, ronan.farrell@mu.ie)

Bill OBrien is with Nonlinear Systems Limited, Dublin, Republic of Ireland (e-mail: bill.obrien@ieee.org). .

Miriam Leeser is with Northeastern University, United States of America (e-mail: mel@coe.neu.edu).

TCAS-I-00328-2019 received March 21, 2019; revised August 01, 2019.

be expressed mathematically in the form

$$PAPR_{dB} = 10Log_{10}\frac{max[(s(t)s^*(t)]}{E[(s(t)s^*(t)]} \quad (1)$$

where E[.] represents the mean of the variable enclosed in the square brackets. Non-linearity of the RF power amplifier (RFPA) would cause amplitude modulation-amplitude modulation (AM-AM) distortion. This in turn requires techniques such as PAPR reduction followed by digital pre-distortion (DPD) for linear operation.

In [1], the authors mitigate the impact of time variant behaviour of the channel by using the application layer traffic information for key generation and have experimentally validated the scheme using SDR (Software Defined Radio) modules. This can serve to mitigate the impact of AM-AM distortion to a limited extent but its effectiveness when applied to probing signals received from transmitters subject to PAPR reduction schemes is currently not clear. In [5], the phase response of the channel between two authentic nodes is probed and is used for encryption key generation. This provides a greater degree of secrecy in comparison with schemes that involve RSSI (Received Signal Strength Indicator) figures due to greater sensitivity of phase to signal propagation path. The probing signal here is also OFDM modulated whose high PAPR would cause AM-PM (Amplitude Modulation-Phase Modulation) when passed through a non-linear RFPA. This would introduce an uncertainty in the phase perceived by the receiver. The authors propose to quantize the received phases to nearest fixed values to mitigate the effect of non-ideal channel which is not exactly reciprocal. This can help to mitigate the problem with AM-PM distortion to a limited extent but experimental validation with hardware has not been performed to test its effectiveness. In this paper, we expand the idea of generating physical layer encryption information published in the above prior arts to include the practical non-ideal hardware and channel aspects that affect the key generation process and evolve a scheme to further strengthen the secrecy of the channel encryption data.

The above schemes focus on scrambling the data such that the data interpreted by the eavesdroppers from the received bit-streams is erroneous. Schemes such as directional modulation (DM) [10], [13], [14] and fast polarization hopping [12] impair the ability of an eavesdropper to receive the transmitted modulation symbols. The scheme proposed in this paper aims to complement the above schemes aimed at impairing the ability of eavesdroppers to receive the transmitted symbols to strengthen the security further.

The problem with PAPR mentioned above has been mitigated in multiple ways involving time domain techniques such as clipping and companding and frequency domain techniques such as SLM (Selective Mapping) [15], tone injection [16], optimized constellation modification [17] and PTS (Partial Transmit Sequence). In [18], the authors accomplish both physical layer security and PAPR reduction for optical communication through the use of chaotic sequences generated using a two dimensional logistic mapping.Each OFDM frame is encrypted U times with U encrypting chaotic sequences. The encrypted OFDM symbols are accompanied with pilot symbols which

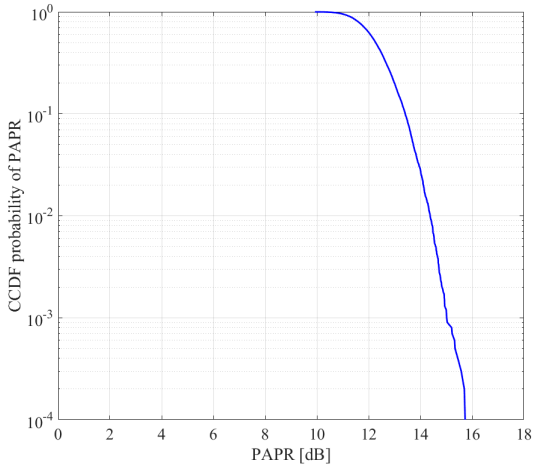

Fig. 1. CCDF plot of a 2048 point OFDM signal with 1664 QPSK modulated sub-carriers exceeding threshold PAPR values

contain the labels of the encrypting sequence. In this paper we expand the concept in [18] to provide PAPR reduction and Physical Layer encryption in wireless communications together without the need to transmit labels and using mutually known information generated through convolved channel and hardware responses. The eavesdropper is obfuscated due to the combined impact of circuit and channel impairments on the probing signal.

Communications in the millimeter wave band involve wide bandwidths and multiple modulation schemes which are selected adaptively depending on the channel state and available resources. Advanced wideband communications employing OFDM schemes such as 5G-NR feature channel bandwidths up to 400 MHz in Ka-Band with FFT sizes up to 4096. This indicates a high probability of PAPR increasing above 10dB. The bandwidth dependent impairments such as ripple and tilt in gain and group delay become significant with increasing signal bandwidths. These are caused by critical blocks in a transmitter such as digital to analogue converters (DACs), mixers, band pass filters (BPF) and amplifiers whose non-uniform gain and phase responses over the channel bandwidth need to be compensated to maintain the integrity of the modulated signal being transmitted. This can be accomplished by means of a feedback receiver at the output of the transmitter's RFPA, evaluate the impairments and generate wideband compensation data which when applied to a wideband modulated signal will pre-compensate it to mitigate the impairments. It is proposed to exploit the frequency response of such non-ideal hardware along with channel response to generate encryption information for the constellation. The encrypted constellation is used to exchange bit level encryption keys as per Diffie Hellmann scheme. [19]. An example of Diffie Hellmann key exchange is summarised in 2. While the scheme is novel, it is critical to ensure that the key exchange does not take place with an impersonating attacker. The physical layer encryption scheme proposed in this paper increases immunity to impersonation attacks during the key exchange process.

In [20], a security scheme exploiting the parameter group

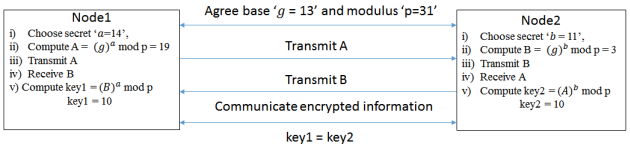

Fig. 2. Example of Diffie Hellmann Key Exchange

delay (GD) to secure the physical layer was proposed. The work presented in this paper provides a novel extension to accomplish encryption of modulated signals to provide security together with reduction of PAPR in OFDM schemes.

1) A scheme to generate encryption keys using the channel characteristics between two legitimate nodes in convolution with the circuit characteristics of the transmitting hardware at the two nodes.
2) A legitimate node transmits a constant envelope stimulus without pre-compensating the signal to mitigate its circuit impairments. The second legitimate node receives the transmitted signal and measures the impairments in it which is a convolution of the channel and circuit characteristics of the transmitter at the first node. The second node re-transmits the stimulus without pre-compensating the stimulus to mitigate its circuit impairments. This is received by the first node which measures the channel characteristics convolved with the circuit characteristics of the second node.
3) Each node then convolves its own circuit characteristics with characteristics evaluated from the received signal. This leads to symmetric information at both the legitimate nodes to generate the modulation encryption keys. The eavesdropper would find it difficult to distinguish the circuit characteristics from channel characteristics by evaluating the signals it received.
4) The modulation encryption key is used to generate frequency domain phase offsets which disperse the phases of the signal's constituent frequency components thereby encrypting it.
5) The two nodes agree values for base 'g', modulus 'p' and exchange A = (g^a)mod p and B = (g^b)mod p respectively over the wireless link through modulation encrypted signals. Each node the computes symmetric keys from the received values of A and B by computing (B^a) mod p and (A^b) mod p respectively to yield the bit encryption keys.
6) The proposed dispersion of phases in the frequency domain also reduces the PAPR of OFDM signals.
7) The entire scheme system has been experimentally validated successfully with zero BER (Bit Error Rate) at the legitimate receiver.

The remainder of this paper is arranged as follows: In Section II we describe the proposed scheme of concealing the air interface parameters by introducing constellation distortion in the modulated signal with calculated amounts of non-linear phase or GD variation across the occupied bandwidth and its inverse operation at the authorized receiver to recover the original modulated signal. Experimentally measured results at 28.9 GHz to validate the technique are presented in Section III. Finally in Section IV we present the main conclusions from this work.

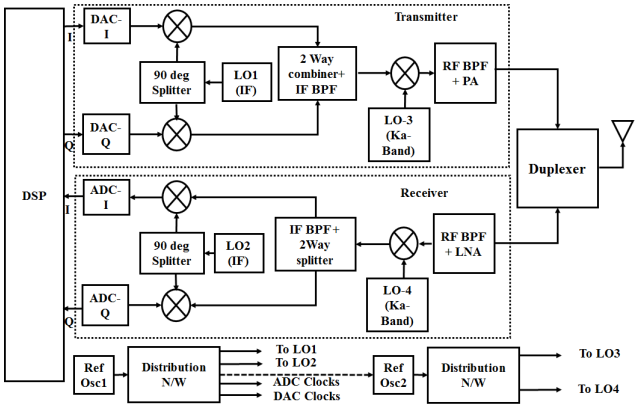

Fig. 3. Generalized Block diagram of a wireless transceiver

II. System Design

The generalised block diagram of a wireless transceiver is shown in Fig. 3. In the transmitting section, the digital signal processor (DSP) performs the task of vector modulation symbol generation, baseband filtering, digital up-conversion (optional), baseband filtering, quantization and yields the in-phase I and quadrature Q components of the intended digital baseband modulated signal. These signal components are then applied to digital to analogue converters (DACs) whose outputs are vector up-converted to an intermediate frequency (IF), further up-converted to the intended RF carrier frequency, amplified and subsequently transmitted. The non-ideal characteristics of these hardware blocks such as sinc-roll off in DACs, amplitude ripple, tilt and group delay in the amplifiers, mixers and filters respectively result in non-uniform gain and phase responses to wideband signals. These impairments would need to be compensated by means of a calibration process to maintain the integrity of the modulated signal being transmitted in addition to AM-AM and AM-PM characteristics of the RFPA. The AM-AM and AM-PM distortion may be considered negligible if the envelope of the input signal is constant.

In the receiver, the signal sensed by the antenna is subject to low noise amplification by the RF low noise amplifier (LNA), down-conversion to an intermediate frequency, further vector down-conversion to extract the I and Q baseband components which are digitized in the analogue to digital converter and applied to the DSP for digital demodulation and further processing. The wide band non-uniform gain and phase responses are also observed in the receiving blocks. This also requires calibration over the band of interest to maintain the integrity of the received wideband signal.

In a typical digital wireless communication scenario, the digital data input to the transmitter is already encrypted/encoded in accordance with the protocols defined in the upper layers of the network stack. One of the ways to further reduce the probability of interception is to conceal the

modulation parameters of the transmitted signal by introducing a known amount of distortion in the constellation with a controlled parameter, the parameter is in turn set using a secret key known only to the authorised nodes. We propose to accomplish this task by distorting the phases of the modulated symbols in a controlled and reversible manner.

A. Key Generation scheme in TDD systems

This case represents the potential application scenarios in small cells and short range wideband millimetre wave wireless communications. The key generation in this case exploits channel reciprocity between two legitimate nodes. Practically, a channel is never reciprocal but may be assumed reciprocal within the channel coherence time. This time interval is dependent on the frequency of operation, environmental fading and Doppler effect in the channel of operation. The first step is to let the two legitimate nodes probe the channel. The probing signals are required to be shorter than the channel coherence time T_c.

$$T_c = \frac{9}{16\pi f_d} \tag{2}$$

$$f_d = \frac{vf}{c} \tag{3}$$

where f_d is the Doppler frequency, f is the carrier frequency of operation, c is the velocity of propagation of an electromagnetic wave in free space and v is the radial velocity between the nodes in m/sec. The duration of the probing signal and the propagation time between the communicating nodes needs to be significantly lower than the channel coherence time Tc. In a time division duplex (TDD) system, the transmission is half duplex implying that only one node can transmit in a given time-slot. Therefore, the combined signal duration and propagation delays for channel probing by both nodes needs to be significantly lower than the channel coherence time. Prior art mentioned in Section I use OFDM signals to probe the channel. One of the problems encountered with OFDM signals for probing is their varying envelope with a high peak to average power ratio (PAPR) as explained in the previous section. This signal when amplified by non-linear power amplifiers in the transmit chain would result in distortion in the probing signal itself before the digital linearization blocks in the transmitter act to linearize the power amplifier. An alternate approach is to use a probing signal whose envelope is constant and has a bandwidth equal to or greater than the channel bandwidth of interest. One such signal is a frequency modulated chirp signal described mathematically in (4) and (5) where $y(n)$ is the value of the nth sample, T_s is the sampling interval, M is the total number of samples, k is the frequency variation parameter, f_{max} and f_{min} are the maximum and the minimum frequencies respectively. Another advantage of a chirp signal exploited in this work is its relative higher immunity to channel noise. The received signal at the legitimate nodes can be subject to piece-wise analysis since the spectral content of each piece is distinct and does not overlap with other the spectral content of other pieces.

$$y(n) = \sin\left\{2\pi\Big(\frac{knT_s}{2} + f_{min}\Big)nT_s\right\} \tag{4}$$

$$k = \frac{f_{max} - f_{min}}{M} \tag{5}$$

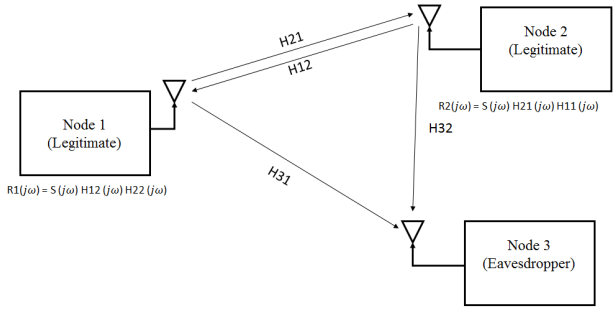

Fig. 4. Channel model for probing

The duration of the probing signal is MT_s. This needs to be chosen such that the sampling interval is lower than the Nyquist rate for the intended bandwidth and the overall signal duration is significantly lower than half of the channel coherence time. The two nodes also need to be synchronised in time so that they transmit without collision at the appropriate time slots. The wireless channel model for probing is shown in Fig. 4. Assuming the following conditions with our wireless communication link we can derive the procedure to probe the channel characteristics convolved with the circuit characteristics of the transmitting node.

1) Node 1 and Node 2 are the legitimate nodes and Node 3 is an eavesdropper.
2) The legitimate nodes have their clocks and timing circuits synchronized with a common reference source such as a GPS. A timed interrupt logic runs on each node to enable transmission.
3) The carrier phases of the local oscillators (LOs) are synchronized with GPS disciplined oscillators or similar reference sources.
4) The hardware signal paths in the receive section of each node are calibrated to mitigate hardware impairments such as IQ phase offset, IQ gain imbalance, etc using techniques described in [21] or similar. The hardware signal paths in the transmit section of each node are not calibrated for wideband gain and phase variations.
5) The impact of RFPA non-linearities such as AM-AM and AM-PM distortion on the constant envelope probing signals is negligible.

The proposed procedure to probe the channel response is summarised in Fig. 5. First we let Node 1 initiate the probing by transmitting a predefined chirp signal described by (4) at time interval T1; Node 1 switches to receive mode after transmission. Node 2 is maintained in receive mode till time interval T2.

$$T2 > T1 + T_{sym} + T_p + T_g \tag{6}$$

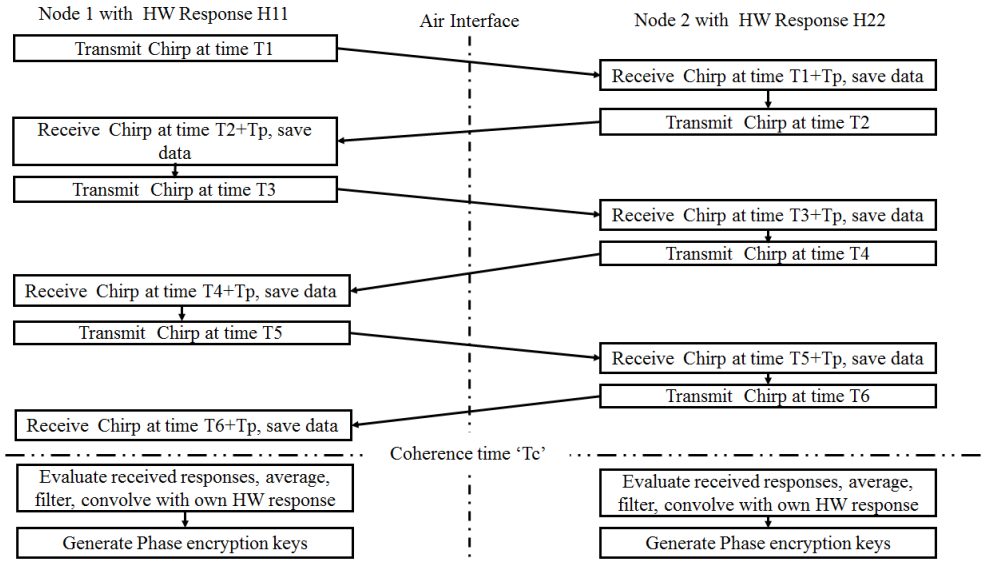

Fig. 5. Key generation work flow for TDD systems.

where, T_{sym} is the probe signal duration, T_p is the propagation time, T_g is the guard interval and $T_g \leq T_p$. Node 2 receives the transmission from Node 1 until time T2 and transmits the pre-defined chirp pulse at time T2. Node 1 receives the transmission from Node 2 during this period until time interval T3 where T3-T2 = T2-T1.

This is repeated at time slots T3, T5 and T4 and T6 respectively. $T6 - T1 < Tc$ (channel coherence time). The received magnitude responses are normalised to the peak amplitude values observed in each time slot and are averaged. The averaged response r2 received by Node2 is an ideal Chirp signal y(n) convolved with the impulse response h11 of Node1's transmitting hardware and the impulse response of the channel h21. Similiarly, averaged response r1 received by Node1 is an ideal Chirp signal y(n) convolved with the impulse response h22 of Node2's transmitting hardware and the impulse response of the channel h12. The fast Fourier transform (FFT) of the averaged responses is computed at both nodes for ease of analysis. The FFTs may be expressed as in the equations below.Since the receivers in the nodes are calibrated, their hardware responses may be absorbed into H21 and H12.

$$R2(j\omega) = Y(j\omega)H11(j\omega)H21(j\omega) \tag{7}$$

$$R1(j\omega) = Y(j\omega)H22(j\omega)H12(j\omega) \tag{8}$$

Node2 then de-convolves y(n) from r2 and convolves the result with its own transmitting hardware's impulse response h22 to yield e2 ($E2(j\omega)$ in frequency domain). Node1 then de-convolves y(n) from r1 and convolves the result with its own transmitting hardware's frequency response h11 to yield e1($E2(j\omega)$ in frequency domain). If H12 = H21, then E1 = E2 as can be seen from the equations below.

$$E_2(j\omega) = \frac{R_2(j\omega)}{y(j\omega)}H_{22}(j\omega) \tag{9}$$

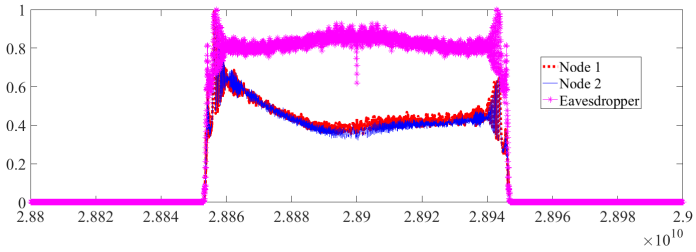

Fig. 6. Normalised Convolved Channel and Hardware Frequency Responses

yielding

$$E_2(j\omega) = H_{11}(j\omega)H_{21}(j\omega)H_{22}(j\omega) \tag{10}$$

$$E_1(j\omega) = \frac{R_1(j\omega)}{y(j\omega)}H_{11}(j\omega) \tag{11}$$

yielding

$$E_1(j\omega) = H_{22}(j\omega)H_{12}(j\omega)H_{11}(j\omega) \tag{12}$$

The above scheme aims to generate symmetric encryption keys at both nodes with asymmetric transmitted information. The eavesdropper Node3 will be able to receive the transmitted chirp signals but will not be able to distinguish the impairments caused by the channel from that caused by un-calibrated transmitting hardware at each legitimate node. The key scheme presented in the paper is comparable with the Diffie-Hellmann key exchange scheme [22]. Since the transmission of the chirp signals is controlled by timed interrupts, response by the eavesdropper Node3 to the stimulus from Node1 will accompany the response from Node2. This can delay the agreement of symmetric keys between Node1 and Node2 but Node3 will not be able to get the key data.

In a practical scenario, E1 will not be equal to E2 owing to noise, variations in performance of receiving hardware and measurement errors but will be highly correlated showing similar trends. A shifted fast fourier transform (FFT) plot

of convolved channel and circuit characteristics computed over a bandwidth of 100 MHz at a carrier frequency of 28.9 GHz is shown in Fig. 6. The evaluated responses E1 and E2 are subject to moving median filtering of a pre-determined window length to mitigate the effect of noise and receiving hardware introduced impairments. One of the ways to extract symmetric data for encryption is to perform non-linear curve-fitting on sections of the computed responses and to use the evaluated coefficient values for key generation. For example, the filtered responses may be classified into regions depending upon change of slope of the frequency response and each region is subject to piece-wise non-linear curve-fitting operations applying the method of least squares. In Fig. 6, the responses in the frequency band 28.85 GHz to 28.86 GHz show a rising slope. This may be classified as a region. Similarly, the responses in the bands 28.6 GHz to 28.9 GHz, 28.9 to 28.92 GHz, 28.92 GHz to 28.94 GHz and 28.94 to 28.95 GHz may be classified as four more regions after being subject to moving median filtering operation to mitigate the impact of noise. The responses in the above regions may be subject to curve-fitting operation applying the method of least squares in accordance with equation

$$y(n) = ax^3 + bx^2 + cx + d \tag{13}$$

The ratio of the curve-fitting coefficient values are computed, rounded off to nearest integer values and quantized to nearest prime numbers to yield a set of encryption keys which may be designated as key1.

The filtered responses are then divided into a convenient number of regions or sub-bands of equal lengths and classified on the basis of signal power distribution. For example, the convolved frequency responses over a bandwidth of 100 MHz computed at each node is shown in Fig. 6. This may be divided into 8 sub-bands of bandwidth 12.5 MHz each and may be numbered in descending order according to the measured power in each sub-band. The range of indices or frequency bin numbers denoting each region are extracted and the highest prime number in each region is extracted. For example, if the responses were sampled at a frequency of 200 MHz and the FFT was computed with 2048 frequency bins, a bandwidth of 100 MHz would occupy 1024 frequency bins with each bin representing a frequency resolution of 97.65625kHz and each sub-band of 12.5MHz bandwidth would occupy 128 points in the FFT space. Fig. 6 represents a shifted FFT plot where the band of interest lies between FFT bin numbers 513 to 1537. The sub-band of 12.5 MHz having the highest band power would occupy the frequency bins from 641 to 768. The highest prime number in this band 761. This will be the first element of second key set designated as key2. Similarly, the highest prime number in the band with the next highest band power is extracted and is stored as the second element of key2. This continues till all eight elements of key2 are extracted. The sequence in which the prime numbers are entered in the space of key2 is critical. The key sets key1 and key2 are expected to be the same at the legitimate nodes Node 1 and Node 2 due to highly correlated responses and different at Node 3. This can be inferred from Fig. 6 which shows plots of experimentally determined convolution of frequency responses of the channel the hardware at 28.9 GHz over a bandwidth of 100 MHz.

The encryption data extraction procedures mentioned above are not exhaustive and there can be several other ways of extracting symmetric encryption keys depending upon the application.

A subset of prime numbers is chosen from both the keys and applied as coefficient values to a non-linear function such as an elliptic function to derive a set of phases for encryption of the spectral characteristics of the modulated signal to be transmitted by dispersing its phases. The encrypting symbols and the phases are updated with new values after convenient intervals using different non-linear functions and a different set of prime numbers from the two key sets to maintain security against brute force attacks and avoid letting the adaptive equalizers in the eavesdropping nodes learn the encrypting information.

The effectiveness of encryption is proportional to the number of secret bits that can be generated by channel probing. But this value is limited by the channel noise and dynamic range of the hardware modules in the transceivers at the communicating nodes. But the encryption information generated so far would be suitable to authenticate a stronger key generation process. A Diffie-Hellman key exchange scheme is initiated to increase the security against brute force attacks. The values of modulus and base are either pre-determined or transmitted from Node 1 to Node 2 over through modulation encrypted signals.The encrypted modulation symbols proposed authenticate the genuineness of the probing nodes and increase immunity against impersonation attacks. Node 1 and Node 2 then exchange the preliminary keys A and B through modulation encrypted signals. Each node then computes the bit level encryption keys as illustrated in 2. The data to be communicated is first encrypted at bit level using the bit encryption keys, modulated in baseband, subject to encryption of the modulated constellation and transmitted. The process is reversed at the receiver to recover the transmitted data. The length of the bit encryption key is chosen to be at least 512 bits.

B. Encrypting the constellation in Single Carrier systems

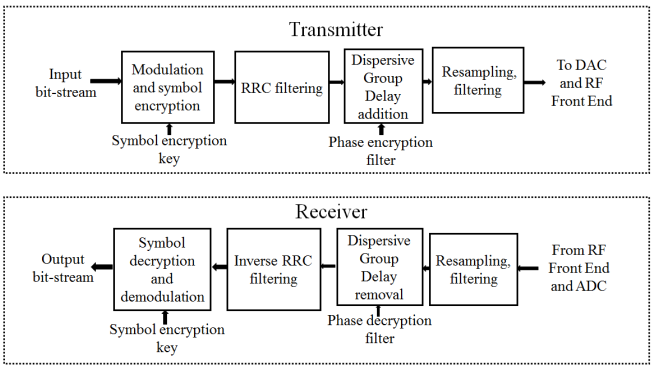

Fig. 7. Proposed Physical Layer Encryption Scheme with Encryption Filter

A key parameter of the physical layer components that can have an adverse impact on the integrity of the modulation

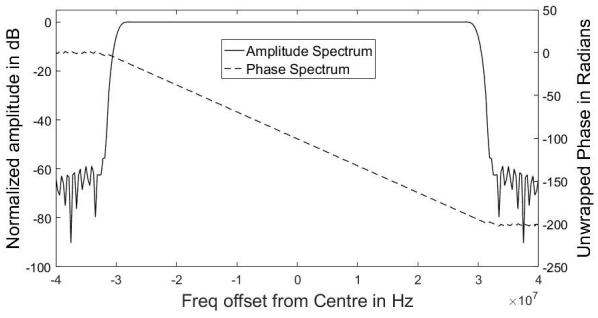

Fig. 8. Frequency Response of a Hamming Windowed Filter

symbols transmitted is the group delay (GD) variation over the bandwidth of interest. Group delay is defined as the rate of change of phase with angular frequency.

$$GD = \frac{d\theta}{d\omega} \tag{14}$$

where GD is the group delay in seconds, θ is the phase in radians and ω is the angular frequency in radians/second. It is a parameter that refers to the dispersion of the individual frequency components that constitute the spectrum of the desired modulated signal. Experimental results in [23] indicate that a significant amount of constellation distortion is introduced in a QPSK modulated carrier if a parabolic group delay variation higher than 1.15 times the symbol duration T_s is introduced. This can be exploited to provide security in the physical layer of a single carrier wireless communication system by means of a programmable dispersive filter.

The spectral characteristics of single carrier modulated signals can be encrypted using dispersive filters to distort the modulation phases. A dispersive filter is one which exhibits a non-linear phase response or group delay in the frequency domain. Such a filter can be designed in the digital domain by manipulating the phase response of a Finite Impulse Response (FIR) filter in the frequency domain to have the required non-linear phase variation for encryption.

Finite Impulse Response (FIR) filters are preferred in the area of digital baseband filtering due to the flexibility available in shaping the spectral characteristics. FIR filter kernels are usually designed to exhibit a near flat amplitude response and a linear phase response over the bandwidth of interest. An example of an FIR filter that meets this criterion is a Hamming window based truncated Sinc filter whose impulse response is defined by the kernel:

$$h(n) = \sin \frac{2\pi f_c(n - \frac{M}{2})}{n - \frac{M}{2}} \left(0.54 - 0.46\Big(\frac{\cos(2\pi n)}{M}\Big) \right) \tag{15}$$

Where f_c is half of the intended bandwidth of the modulated signal, M is the sample length of the truncated Sinc kernel, n is the sample number ranging from 0 to M whose value is selected depending upon the desired transition region between the pass and stop bands. The FFT or frequency response of this filter is as shown in Fig. 4. This filter exhibits a linear phase response or constant group delay. This filter can be made dispersive to encrypt the spectral characteristics of the signal to be transmitted by introducing a non-linear characteristic in the phase of its frequency response or FFT.

The design procedure for the encryption filter is similar to that described in conference paper [20] as explained in the following steps.

1) Obtain the symbol rate, occupied bandwidth (BW) and modulation constellation of the modulated carrier intended to be transmitted.
2) Calculate the minimum variation in GD over the bandwidth of interest needed to cause constellation distortion using the mathematical relation:
$$\frac{GD}{T_s} \geq 1.15 \tag{16}$$
3) Calculate the peak variation $d\theta_{max}$ required in the phase response by equating $d\omega$ in equation (14) to BW noted in step 1 and using the value of GD obtained in step 2.
4) Design a FIR filter kernel for the intended i.e. occupied bandwidth of the modulated signal using the kernel defined in equation (15). Obtain the FFT of the filter designed, extract the amplitude and phase values of the resulting spectrum.
5) Calculate the number of points occupied by the bandwidth of interest in the FFT plot. For example, if the bandwidth of the signal of interest is 160 MHz, generated digitally at a sample rate of 640 MHz and if the number of points chosen for the FFT is 1024, the number of FFT points occupied by the signal of interest would be 256. Since FFT is a two-sided spectrum, half of the frequency components would occupy the position from 1 to 128 and the other half would occupy the points 897 to 1024 in the example considered.
6) The prime numbers chosen from the first and second key sets are used as coefficient values of parameter x to provide encryption phases y in a non-linear mathematical function such as an elliptic function in the form.
$$y = p^2 = mod(x^3 + f_1 x + f_2, f_3) \tag{17}$$
Where f_1, $f_2$and f_3 are three prime numbers selected by a symmetric algorithm from the two key sets,x is the frequency bin number, p^2 is the outcome of the non-linear mathematical operation for a given value of x that yields the encrypting phase value designated as y. One of the challenges in designing the group delay variation curve for single carrier schemes is that the variation needs to be continuous to maintain the integrity of the signal's envelope. This is accomplished by subjecting the values of y in (17) to raised cosine filtering.
7) The encryption phase values are added to the phases of the FFT of a pre-determined FIR filter and its IFFT is derived to yield the encrypting filter. The phases of the encrypting filter in FFT domain are inverted and subject to IFFT operation to yield the decrypting filter. This completes the design of encryption and decrypting filters to conceal and recover the modulated constellation respectively. These filters are expected to be identical at the two legitimate nodes.

The encryption of the modulated constellation is accomplished by convolving the modulated baseband with the encryption filter at the transmitter in the digital domain prior to conversion to analogue domain and transmission. The recovery of the encrypted modulation symbols is accomplished by convolving the encrypted baseband signal with the decryption filter in digital domain at the receiver.

The generated keys are first tested for symmetry with random data where Node 1 generates a set of random bits and modulates them on to the intended constellation 8PSK for example. These symbols are subject to encryption at symbol level through modulo addition with the first key. The encrypted symbols are subject to the necessary re-sampling, pulse shaping (Root Raised Cosine filtering for example) depending on the modulation standard and then convolved with the encrypting filter. The encrypted baseband is transmitted after the other necessary signal processing operations. Node 2 receives the signal transmitted by Node 1, digitizes it, applies noise filtering and subjects the baseband to decryption filtering to recover the modulation constellation. The recovered baseband is then subject to equalization to compensate for channel impairments. If the recovered modulation phases at this stage do not correspond to standard values within an agreed deviation limit, a failure message is sent to Node 1 and the entire key generation process restarts. Else, the recovered baseband modulation symbols are demodulated to recover the transmitted symbols. Node 2 remodulates the recovered symbols on to another baseband with the same modulation scheme, encrypts the phases with its key and re-transmits it. Node 1 now receives, decrypts and demodulates the data to recover the bit-stream and compares it with that it transmitted. If a match is found, a success message is transmitted to Node 2. This completes the phase encryption key generation and agreement process along with the design of symmetric encryption and decryption filters. It may be noted that no confidential data is transmitted until this stage.

The encrypting phases and symbols are updated to new values at both nodes by running a common algorithm that selects different non-linear functions and different sub-set of key values symmetrically at both nodes after a definite interval of time has elapsed. This is done through timed interrupts.

A second signal transmission of random bits without encryption could be used to estimate the channel to aid in equalising the gain and phase impairments suffered by the first signal. It may be noted that no confidential information is transmitted until now. The proposed physical layer encryption and decryption process at the transmitter and receiver of each node to secure the communication is summarized in Fig. 7.

C. Encrypting OFDM systems

A subset of prime numbers chosen by a symmetric algorithm from the two key sets are applied as coefficient values in a non-linear function to generate encrypting phases. The positions of the prime numbers in the non-linear function are interchanged and the non-linear function is executed again to obtain a convenient number of encrypting phase sequences. The sequence with maximum variance is chosen to encrypt the

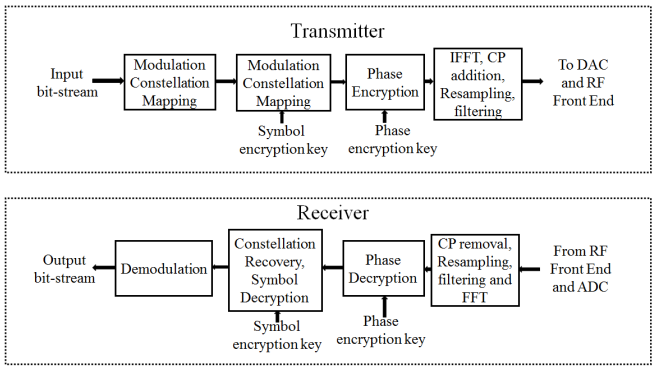

Fig. 9. Proposed PHY encryption and decryption in the transmitter and the receiver of OFDM systems

OFDM symbols to minimise PAPR. Unlike the single carrier schemes, each modulated symbol is transmitted on a sub-carrier in OFDM modulated signals. Therefore the encrypting phases thus generated are added directly as offsets to the phase of each sub-carrier. This method is computationally more efficient than convolving the signal in time domain with a dispersive filter. Three phase sequences were generated in the experimental validation of this technique and their element-wise product was taken to maximise variance. Randomisation of phases of the sub-carriers in an OFDM modulated signal reduces its PAPR [15] along with providing security of information [18]. This is an enhancement over prior art where modulation phase of each sub-carrier including the pilot is encrypted.

The generated keys are first tested for symmetry as explained for the single carrier case except that the the encrypting phases are added and subtracted directly at the transmitting and receiving nodes instead of convolving with FIR filters. The proposed physical layer encryption and decryption process at the transmitter and receiver of each node to secure the communication in OFDM systems is summarized in Fig. 9.

The procedure for key generation illustrated above is applicable to TDD systems. The reciprocity of channel response is not applicable to Frequency Division Duplex (FDD) systems and it is therefore imperative to consider other parameters for symmetric key generation. This is intended to be taken up as future work.

III. Experimental validation

The experimental validation was conducted for an 8PSK signal case of bandwidth 100 MHz and for a QPSK-OFDM signal of the same bandwidth. The transmitter and the receiver were built as per the block diagram shown in Fig. 3 for transmission at carrier frequency 28.9 GHz. The IF in the transmitter was selected at 600 MHz which was then up-converted to 28.9 GHz. LO3 and LO4 were set at 14.15 GHz and were multiplied in frequency by a factor of 2 owing to better phase noise performance than using an oscillator directly at 28.3 GHz to mix with the IF at 600 MHz to yield the modulated carriers at 28.9 GHz at power +2 dBm. The receiver consisted of an RF front end with a noise figure around 3 dB and gain of 13 dB which down-converted the

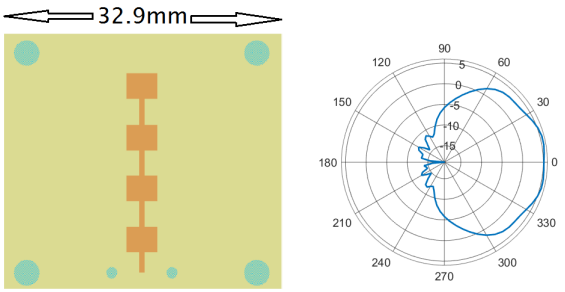

Fig. 10. Gerber screenshot of the antenna designed and its simulated gain pattern (dBi) in azimuth plane.

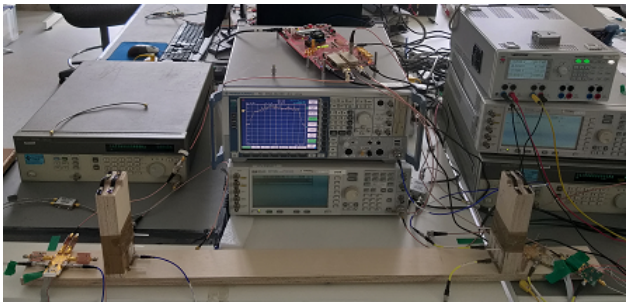

Fig. 11. Test Bench used for validation. Node 1 is on the left. Node 2 and Node 3 are on the right. Node 3 is connected to a Vector Signal Analyzer.

received signal to an IF at 600 MHz. This was followed by an analog to digital converter (ADC) clocked at 4 Gsps that digitized the IF. Further down-conversion and demodulation were accomplished in the digital domain. The antennas were designed to have beam-widths of 120 degrees in the azimuth plane as shown in Fig. 10 and etched on RO3003 substrate from Rogers Corporation. An IF amplifier with a gain of 10dB was used in the receiver section of Node1 and no IF amplifier was used in the receiver section of Node2 to introduce hardware differences at the two nodes which would introduce differences in the noise figures at the two nodes.

A. Modulation Encryption Key Generation

A wooden test apparatus was designed with propagation path length of a meter between its ends. This distance corresponds to 96 wavelengths at 28.9 GHz. One of the ends of the apparatus was mounted with a patch antenna and termed Node 1. Two additional antennas were fabricated on a similar substrate for Node 2 and Node 3 at a spacing of eight wavelengths with a ground plane in between them. Node 2 was termed the second legitimate node and Node 3 was designated to be the eavesdropper. An overall path loss of 51 dB was observed between the legitimate nodes. The evaluation was performed in a regular laboratory environment instead of an anechoic chamber to emulate a real use case scenario that would include multipath propagation effects. A picture of the test bench is shown in Fig. 11.

The first task was to calibrate the receiver sections of the two legitimate nodes for flatness of frequency response. This was done using a calibrated signal generator SMW200A of Rohde and Schwarz by sweeping the frequency of an input

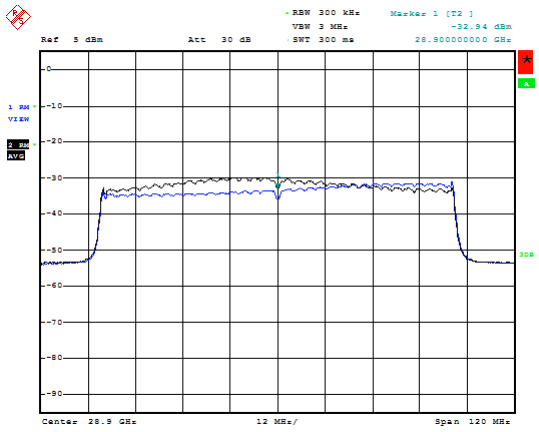

Fig. 12. Frequency Responses of Node1 and Node2 at 28.9 GHz

single tone sine wave from 28.8 GHz to 29 GHz in steps of 5 MHz and recording the variation whose values were used to build an FIR filter to calibrate the frequency response. The next task was to determine the hardware frequency responses of the two nodes over the band of interest. The RF output of each node was connected to a calibrated spectrum analyzer (FSQ40 Vector Signal Analyzer from Rohde and Schwarz). A screenshot of the un-calibrated hardware frequency responses of Node 1 and Node 2 captured on the spectrum analyser is shown in Fig. 12.

The third task was to measure the extent of reciprocity of the channel response between Node 1 and Node 2 (legitimate) and the channel response between Node 1 and Node 3 (eavesdropper). The frequency responses of the transmitting sections of the nodes were measured and recorded in the form of an FIR filter. This was done by taking the element-wise ratio of response to stimulus in frequency domain (FFT) and multiplying the ratios with the frequency response of a hamming window defined in (15).The procedure for this task is detailed in [21]. The inverse transfer function of this FIR filter was derived for each node in the form of another FIR filter to calibrate the transmitting hardware over the bandwidth of interest. Node 1 was configured to receive and Node2 and Node3 were made to transmit a chirp pulse of duration 3.125x10-6 secs at alternate time intervals after the transmitter in each node was calibrated. The sample rate chosen was 640 MSPS. The down-converted IF output of Node1 was connected to a spectrum analyser and the responses were observed with the traces saved. Node1 was now configured to transmit and Node2 was configured to receive and its down-converted IF output was connected to the spectrum analyzer. A screenshot of the recorded channel responses is shown in Fig. 13. The channel responses between Node 1 and Node 2 are nearly reciprocal and the channel response between the eavesdropping node Node 3 and Node 1 rolls of at the upper band edge by 2 dB.

Having established the difference in the legitimate and the eavesdropping channels, the next task was to generate symmetric keys between Node 1 and Node 2. The block diagram of the apparatus used is shown in Fig. 14. A PC running MATLAB was used as the DSP and timed interrupt

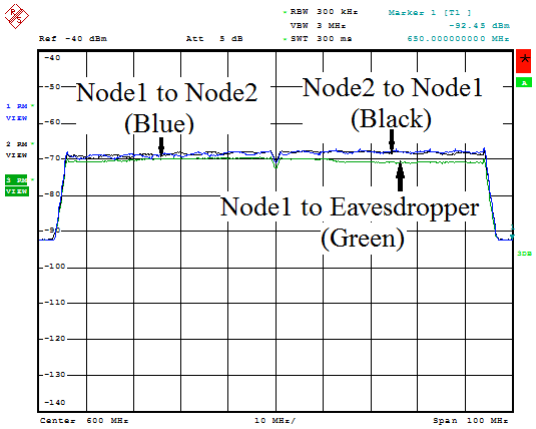

Fig. 13. Screenshot of measured channel responses between legitimate nodes and the eavesdropper

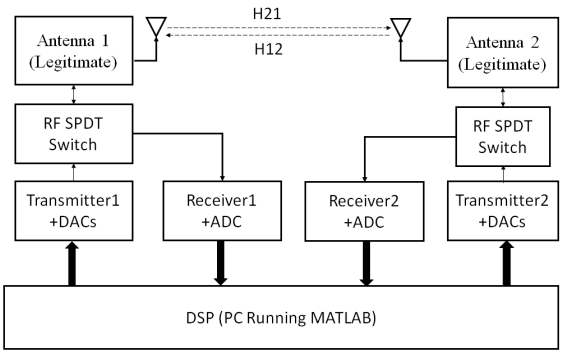

Fig. 14. Apparatus used for symmetric key generation

generator. A pair of DACs followed by a Ka Band transmitter was connected to each of the legitimate nodes Node 1 and Node 2. The receivers and transmitters RF paths were duplexed with SPDT switches. The probe signal chosen was a chirp pulse of duration $3.125\text{X}10^{-6}$ secs with a bandwidth of 100 MHz generated at sample rate 640 MHz. The transmitters at Node 1 and Node 2 were made to transmit thrice at alternate time intervals of $3.125\text{X}10^{-6}$ sec. The first transmission was from Node 1 and the last was from Node 2.

The responses were extracted at the appropriate controlled time slots and saved in separate files for analysis. The responses over three time slots recorded at each node were averaged, filtered, down-converted digitally to zero IF and down-sampled to 400 MSPS. The received signal consisted of a chirp pluse subject to convolution with the impulse response of the channel and the hardware of the transmitting node. The received signal was transformed to frequency domain by an FFT operation to de-convolve the stimulus and the resulting amplitude and phase values were saved in the form of an FIR filter kernel. This was further convolved with the receiving node's own hardware impulse response in transmitting mode. This yielded similar data at both the legitimate nodes whose FFT could be used to derive encryption keys as detailed in Section II.

A bandwidth of 112.5 MHz (100 MHz + additional bandwidth of 12.5 MHz) in a 512 point FFT space sampled at

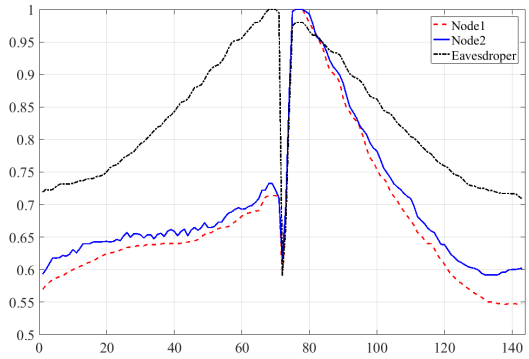

Fig. 15. Key generation information consisting of convolved channel and hardware responses evaluated at each node.

400 MHz would occupy 144 points symmetrically on both sides. The first and last 72 points which contain the convolved responses were extracted, subjected to moving median filtering of span 3 to be used as the basis for encryption at each node. These basis curves were subject to curve fitting operation for key generation. Plots of the normalised basis curves extracted from the convolved circuit and channel responses individually at each authentic node is shown in Fig. 15. The plot of the characteristics measured at Node 2 indicates higher amount of noise. This was due to reduction in the gain at Node 2 which was introduced deliberately to assess the ability to produce symmetric encryption keys i the presence of noise. The effect of noise was mitigated by moving median filtering.

The plotted curve was divided into regions on the basis of change of slope after filtering. Each region was subject to piece-wise curve-fitting operation to a non-linear function of the form $y = ax + bx^3 + cx^5 + d$ by applying the method of least squares on MATLAB. The values at the 14 frequency bins located at the centre of the curves pertaining to band edges in the received responses were ignored. The ratio (d/a)+b was computed in each case. In cases where the values obtained for any of the coefficients were less than 0.1, they were replaced by 0. The ratios $k1_1$ and $k2_2$ obtained at Node 1 and Node 2 when the curves were divided into five regions are as copied below.

$set_1 = \{5.06257,\ -1.49450,\ 0.9875,\ 30.0487,\ -11.475\}$
$set_2 = \{5.20483,\ -1.49222,\ 0.9723,\ 30.0430,\ -10.633\}$

Each of the coefficient values were multiplied by a power of 10 such that there were atleast two digits before a decimal point and the magnitude was rounded off to the nearest prime number which yielded symmetric sets of the first key at the two nodes.

$Node1Key1 = \{51,\ 13,\ 97,\ 31,\ 11\}$.
$Node2Key1 = \{51,\ 13,\ 97,\ 31,\ 11\}$

The key sets Node1Key1 and Node2Key1 generated were identical at the two legitimate nodes.

This was followed by a second key generation task which involved division of the filtered responses into eight regions of equal lengths of 18 data points and evaluating the RMS (root mean squared) of the magnitudes of the normalised responses in each region. The largest prime number of the index in each region was extracted. The extracted prime numbers were

arranged in descending order of the rms value of the region from which they were extracted. The rms values of each region evaluated at Node1 and Node2 are as copied below.

$rmsNode1 = \{0.6209,\ 0.6447,\ 0.6543,\ 0.6830,\ 0.8985,\ 0.7882,\ 0.6563,\ 0.5930\}$

$rmsNode2 = \{0.5719,\ 0.6072,\ 0.6217,\ 0.6504,\ 0.8871,\ 0.7815,\ 0.6351,\ 0.5551\}$

Referring to Fig. 15, one can observe by inspection that the region between data points 73 and 90 would have the maximum rms value. The highest prime number in this region is 89 and hence it would be the first entry in the second key set.

$Node1Key2 = \{89,\ 107,\ 71,\ 113,\ 53,\ 31,\ 17,\ 139\}$

$Node2Key1 = \{89,\ 107,\ 71,\ 113,\ 53,\ 31,\ 17,\ 139\}$

The key sets generated were identical at the two legitimate nodes. The entries in the second key set are just the highest prime numbers in each region but the sequence in which they are entered is critical to generation of the encryption phases. Higher number of entries can be obtained for both the key sets from response curves with higher number of data points. Subsets of 3 prime numbers from the two key sets at the two nodes were selected by a symmetric algorithm to generate the phase offsets needed to encrypt the spectral characteristics of the modulated signal to be transmitted.

In order to assess the extent to which the encryption data could be generated by the eavesdropper, the RF front end section of Node 2 was connected to Node 3 but a different DAC was used in the base-band section. The convolved channel and hardware frequency responses evaluated at Node 3 with the Chirp stimulus eavesdropped from Node 1 is also shown in Fig. 15. This curve is significantly different from that computed at the legitimate nodes and hence would result in different key sets.

Values of base g and modulus p for the Diffie-Hellman scheme were chosen to be 51 and $2^{512} - 51$ respectively. The exponent 'a' chosen at Node 1 was 61 and 'b' chosen at Node 2 was 71. These yielded values of A and B as below. An online tool available at the URL https://apfloat.appspot.com/ was used for computation along with low level file read and write operations since a 512 bit number was beyond the ability of the version of MATLAB available.

$A = 14513786891649432639226333276685646412946467064308075311974716756641217488865306205007092532912453457805 1$

$B = 17277563704993856532212363451596447596623771700684409630436173949266784426333262575344791804129467839402142422442056841051$

These values were converted to bits and transmitted by Node 1 and Node 2 on modulation encrypted carriers in each of the validation case explained below. The raw bit stream was transmitted in each case without forward error correction (FEC) since the distance was small. FEC may be added as needed in field.

B. Encryption of Single Carrier Modulated Signals

The first case of validation was for a single carrier modulation scheme similar to that chosen in [24]. An 8PSK modulated signal of bandwidth 96 MHz was chosen for this case. The symbol rate was set at 80 Msps. The modulated digital baseband was subject to raised cosine filtering with roll off factor α = 0.2 at an oversampling ratio of 4. The resulting sample rate was 320 Msps and the occupied bandwidth was $80\text{x}10^6(1+\ \alpha)$ = 96 MHz.

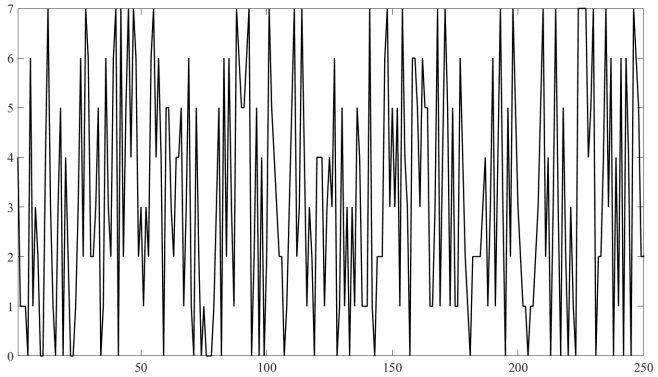

Fig. 16. First 200 encrypting symbols for 8PSK symbol encryption

The minimum in-band nonlinear peak phase variation needed to encrypt this signal calculated as explained in section II was 7.23 radians.

A random bitstream of 18000 bits was chosen to test the symmetry of the constellation encryption keys.The phases for the encrypting filter at Node1 were derived by applying three of the thirteen entries in the key sets Node1Key2 and Node1Key2 as coefficient values in the elliptic function described by 17. The values of f1, f2 and f3 selected for this operation were 47, 89 and 17 respectively to encrypt the first 6000 bits. The values of f2 and f3 were swapped to generate the encrypting symbols for the next 6000 8PSK modulated data symbols and so on to test for symmetry of the constellation encryption keys generated at both nodes.

The first 39 values of the designed phase response were extracted, subject to root-raised cosine filtering with an up-sampling factor of 4 and added to the phases of the FFT of an FIR filter of length 320 described in (15). The IFFT of the modified filter was computed to obtain the encrypting filter at Node 1. The phases of the encrypting filter in the frequency domain were inverted and the IFFT was computed to obtain the decrypting filter at Node2.

The 8PSK modulated data symbols of the random bit-stream were subject to RRC filtering as per DVB-S2 standard, convolved with the encrypting filter at Node1 to conceal its constellation. The encryption and decryption filters were switched after transmission of 6000 symbols to avoid detection of the encrypting phases by an adaptive equalizer in the eavesdroppers. The encrypted signal was transmitted over the air interface at 28.9 GHz, received by Node2, subject to equalization and decryption filtering, down-sampling and recovery of symbols. The recovered symbols were decrypted and the transmitted bit-stream was demodulated without errors. A plot of the received constellation of an 8PSK signal prior to equalization and decryption is shown in Fig. 17. The 8PSK constellation after decryption and channel equalization

is shown in Fig. 18. This task verified the symmetry of the constellation encryption keys.

A VSA (Vector Signal Analyzer) with an internal equalizer based on LMS (Least Mean Squares) was used as the eavesdropping receiver. The length of the equalizer was set at 10 and step size was set at 0.05. The sampling frequency of the VSA was also set at 320 MHz. This implied 40 taps for the internal filter due to an over-sampling factor of 4. The transmission was repeated continuously for five minutes and a faithful recovery of the constellation could not be observed. The length of the equalizer in the VSA was varied from 5 to 20 in steps of 5 and step size was also switched between 0.01 and 0.05 in each case after running for 5 minutes. No faithful recovery of the constellation could be observed in any attempt. All the modulated symbols were then subject to encryption by only the first filter instead of switching between multiple filters. This led to partial identification of the symbols after a learning time of 8 minutes. It was inferred that switching the encryption filter provided tighter security against eavesdroppers. The observations demonstrate that it is essential to use the appropriate decryption filter to first recover the modulation symbols before attempting to demodulate the signal. As the next step, the bitstream for Diffie-Hellman preliminary keys A and B were generated at Node 1 and Node 2 respectively. Since A and B could be of different lengths, zeros were appended in the beginning of the respective bitstreams to make the length l equal to that of the modulus. The resulting bitstream was encrypted with the first l bits from the random bitstream transmitted earlier, modulated on 8PSK symbols and transmitted after encrypting the constellation. The process was reversed at the respective receivers and the transmitted values of A and B were recovered. These were subject to the computation of final keys:

A1 = (B^a)mod p B1 = (A^b)mod p;

A1 = 1118041499078512949486124996043783154132067
940539277973279825585828096851944065463003457048
385063421939335979822511954743411550883009822586
8311167306077536 = B1.

The values of A1 and B1 were used to encrypt and decrypt data bits in further transmissions without errors.

C. Encryption of an OFDM signal

The proposed security scheme was tested on an OFDM system as the second case. A 2048 point FFT based OFDM signal with 1664 active sub-carriers including 128 pilots was generated at sample rate 100 MHz. The modulation chosen for the sub-carriers was QPSK. The data to be transmitted was mapped on to QPSK constellation points on the 1536 active sub-carriers. The amplitudes of all the active sub-carriers were constant since the chosen modulation scheme was QPSK. A constant phase of 45 degrees was chosen for the pilots. The objective here was to encrypt the signal to jointly achieve PAPR reduction and security in the physical layer. The randomization of the phases of the sub-carrier is one of the ways to reduce PAPR [15] [18] for which the selection of the encryption phases at the transmitter and and its knowledge at the receiver are critical. A random stream of

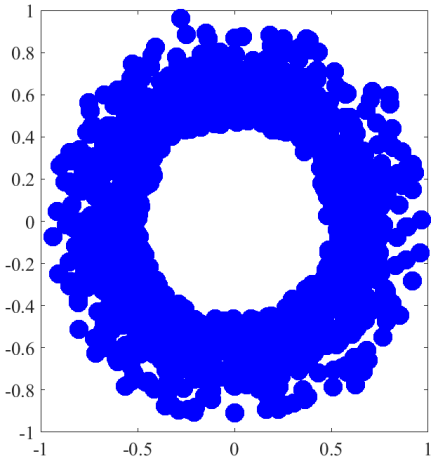

Fig. 17. First 1000 symbols of he received encrypted 8PSK signal before decryption and equalization.

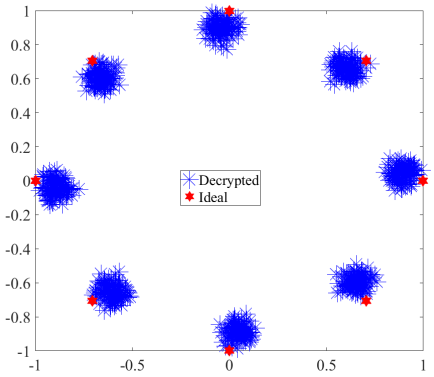

Fig. 18. Recovered 8PSK constellation after decryption filtering and equalization.

3072 bits was generated at Node1 and modulated on the 1536 data subcarriers with QPSK modulation.

$$z_1 = mod(mod(f_1x^3 + f_2x, f_3), 2pi) \quad (18)$$

$$z_2 = mod(mod(f_2x^3 + f_3x, f_1), 2pi) \quad (19)$$

$$z_3 = mod(mod(f_3x^3 + f_1x, f_2), 2pi) \quad (20)$$

$$z_4 = mod(z_1z_2z_3, 2pi) \quad (21)$$

The next task was to generate chaotic phase values to encrypt the spectrum of the OFDM signal. This was done by applying a subset of three prime numbers in the key sets Node1Key1 and Node1Key2.The values of f1, f2 and f3 selected for this operation were 47, 89 and 17 respectively. Three sets of encryption phases each of length 1664 were generated applying the selected prime numbers in elliptic functions as per equations (18, 19 and 20) and a fourth set was generated by taking the element-wise products of the first three sets to modulo $2pi$ as described by (21). The ratio of variance to mean was computed for each set and the phases in the set that had the highest ratio was chosen for encryption. This was computed at both nodes for symmetric encryption

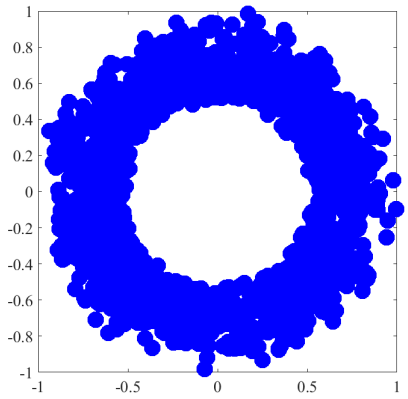

Fig. 19. Phase encrypted OFDM sub-carriers received over the 28.9GHz wireless link.

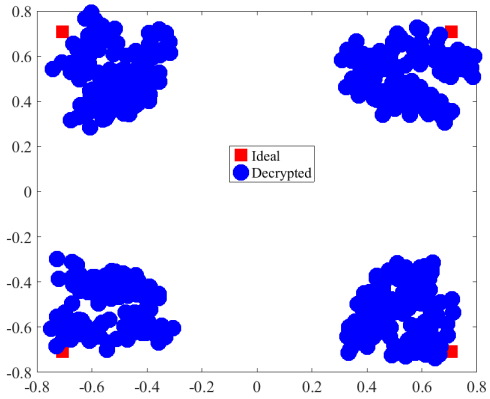

Fig. 20. Recovered QPSK constellation of OFDM sub-carriers received over the 28.9 GHz wireless link.

and decryption. The set z_4 was the best candidate hence the phase values in its set were added to the phases of the 1664 active sub-carriers (excluding null sub-carriers) at Node1 for encryption. A plot of the constellation of the encrypted sub-carriers is shown in Fig. 19. The IFFT of the encrypted subcarriers was computed to yield the time domain signal. A cyclic prefix of 144 samples was appended and the signal was up-sampled by a factor of 2 and transmitted over the 28.9GHz air interface after the necessary signal processing operations. It was observed that the PAPR of the encrypted signal was reduced by 3 dB. This aspect is explored further in the next sub-section. The signal was received at Node 2, down-sampled to the original sample rate after the necessary signal processing operations and the added cyclic pre-fix was removed. The FFT of the received signal was computed and the sub-carriers and subject to decryption of phases. This led to the successful recovery the transmitted constellation. A plot of the constellation of the decrypted sub-carriers is shown in Fig.20. The amplitudes of the sub-carriers were equalized and symbols in the received constellation were decrypted by means of modulo subtraction of the encrypting symbols to recover the original symbols. The recovered symbols were demodulated to recover the original bit stream without errors. As the next task, the preliminary Diffie-Hellman keys A and B were exchanged on the wireless link after appending zeros in the beginning to make the length equal to 3072 bits and encrypting the resulting bit-stream with the random bit-stream exchanged earlier.The process was reversed at the receivers to recover the values of A and B which were then used to compute the values of the final keys A1 and B1 as in the single carrier case. A1 and B1 were used as the encryption and decryption keys for further transmissions. The validation was repeated thrice successfully with different bit streams and encryption keys.

D. PAPR Reduction

The effectiveness of PAPR reduction was tested by measuring the probability of the signal exceeding a threshold value. This may be expressed mathematically by means of a cumulative distribution function [15] of the form (22) where

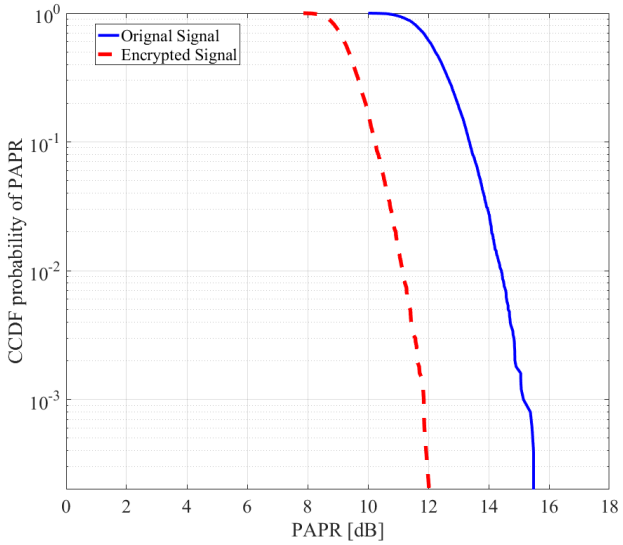

Fig. 21. CCDF of PAPR of Original and Encrypted 2048 point OFDM modulated signals with 1664 active sub-carriers

N is the number of sub-carriers and $PAPR_T$ is the threshold PAPR value.

$$Prob(PAPR > PAPR_T) = 1 - (1 - e^{-PAPR_T})^N \quad (22)$$

Simulations were carried out in MATLAB for 10000 cycles of randomly generated bit streams, modulation and encryption of the subcarriers with the same encrypting phases generated using the encryption key as that used for the validation of the security aspect in the previous subsection. From this it was possible to identify a scheme that would simultaneously reduce PAPR and provide physical layer security. The complex cumulative distribution function (CCDF) plots for the resulting reduced PAPR signal are shown in Fig.21. The proposed scheme reduced the PAPR by over 3.5dB when there is a 2×10^{-4} probability of the original signal exceeding a threshold PAPR of 15.5dB.

IV. Conclusion

In this paper a novel scheme to provide security in the physical layer along with reducing the peak to average power ratio of OFDM signals through dispersion of the phases of the modulated signal has been proposed and experimentally validated. The scheme conceals the modulated constellation from eavesdroppers using symmetric encryption keys which are generated at the legitimate communication nodes exploiting the channel and non-ideal circuit characteristics over the bandwidth of interest. Bit level encryption keys are further exchanged over carriers whose modulations are concealed thereby providing immunity against impersonation attacks. The experimental validation used an end-to-end wireless link at 28.9 GHz which was constructed in-house. It has been demonstrated that the physical layer encryption technique can be successfully reversed at the legitimate receiver on the experimental testbench to recover the original modulated symbols with zero bit errors. The proposed physical layer encryption technique successfully concealed both single carrier and OFDM modulated signals from a well positioned eavesdropper and a reduction of PAPR by 3.5dB was also achieved for an OFDM signal with 1664 QPSK modulated sub-carriers.

Acknowledgment

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant Number 13/RC/2077. The authors would like to thank the reviewers whose valuable feedback helped in improving this work by a significant extent. The authors would also like to thank Mr. James Kinsella and Dr. Somayeh Mohamady of NUI, Maynooth for their assistance in this work and Rogers Corporation for providing the RF substrate RO3003 that was used to fabricate the antennas to validate the proposed scheme . Leeser was funded in part by NSF grant CNS-1836880.

References

[1] B. Z. Katz, C. Sahin, and K. R. Dandekar, "Real-time wireless physical layer encryption," in *2016 IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON)*, April 2016, pp. 1–4.

[2] WiFi pineapple. [Online]. Available: https://www.wifipineapple.com

[3] C. Sahin, B. Katz, and K. R. Dandekar, "Secure and robust symmetric key generation using physical layer techniques under various wireless environments," in *2016 IEEE Radio and Wireless Symposium (RWS)*, Jan 2016, pp. 211–214.

[4] J. Hua, S. Jiang, W. Lu, Z. Xu, and F. Li, "A novel physical layer encryption algorithm based on statistical characteristics of time-selective channels," *IEEE Access*, vol. 6, pp. 38 225–38 233, 2018.

[5] L. Cheng, L. Zhou, B.-C. Seet, W. li, D. Ma, and J. Wei, "Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase," *Mobile Information Systems*, vol. 2017, pp. 1–13, 07 2017.

[6] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Communications Letters*, vol. 19, no. 1, pp. 74–77, Jan 2015.

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409960

[8] W. Hou, X. Wang, J. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[9] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 1276–1284.

[10] Gao Baojian, Luo Yongling, Hou Aiqin, Zhao Xiaoning, and Wu Qian, "New physical layer encryption algorithm based on dft-s-ofdm system," in *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, Dec 2013, pp. 2018–2022.

[11] Y. Ding and V. Fusco, "Improved physical layer secure wireless communications using a directional modulation enhanced retrodirective array," in *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, Aug 2014, pp. 1–4.

[12] Y. Shiu, S. Y. Chang, H. Wu, S. C. . Huang, and H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, April 2011.

[13] Y. Ding and V. F. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 1, pp. 361–370, Jan 2014.

[14] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[15] P. Cheng, Y. Xiao, L. Dan, and S. Li, "Improved SLM for PAPR reduction in OFDM system," in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2007, pp. 1–5.

[16] N. Jacklin and Z. Ding, "A linear programming based tone injection algorithm for papr reduction of ofdm and linearly precoded systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 7, pp. 1937–1945, July 2013.

[17] Y. Kou, Wu-Sheng Lu, and A. Antoniou, "New peak-to-average power-ratio reduction algorithms for multicarrier communications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 9, pp. 1790–1800, Sep. 2004.

[18] W. Zhang, C. Zhang, C. Chen, W. Jin, and K. Qiu, "Joint papr reduction and physical layer security enhancement in ofdma-pon," *IEEE Photonics Technology Letters*, vol. 28, no. 9, pp. 998–1001, May 2016.

[19] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, November 1976.

[20] P. Ramabadran, D. Malone, S. Madhuwantha, P. Afanasyev, R. Farrell, J. Dooley, and B. O'Brien, "A novel physical layer encryption scheme to counter eavesdroppers in wireless communications," in *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, Dec 2018, pp. 69–72.

[21] P. Ramabadran, S. Madhuwantha, P. Afanasyev, R. Farrell, L. Marco, S. Pires, and J. Dooley, "Digitally assisted wideband compensation of parallel rf signal paths in a transmitter," in *2018 91st ARFTG Microwave Measurement Conference (ARFTG)*, June 2018, pp. 1–4.

[22] R. C. Merkle, "Secure communications over insecure channels," *Commun. ACM*, vol. 21, no. 4, pp. 294–299, Apr. 1978. [Online]. Available: http://doi.acm.org/10.1145/359460.359473

[23] A. Azizzadeh and L. Mohammadi, "Degradation of ber by group delay in digital phase modulation," in *2008 Fourth Advanced International Conference on Telecommunications*, June 2008, pp. 350–354.

[24] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1422–1430.