A Novel Physical Layer Encryption Scheme to Counter Eavesdroppers in Wireless Communications

Prasidh Ramabadran, David Malone, Sidath Madhuwantha, Pavel Afanasyev,Ronan Farrell, John Dooley
National University of Ireland, Maynooth
Maynooth, Ireland
prasidh.ramabadran@mu.ie

Bill O'Brien
Nonlinear Systems Limited
Dublin, Ireland
bill.obrien@ieee.org

***Abstract*—Modern wireless communication systems employ wideband modulated RF carriers to communicate the data of interest between the nodes in the network. The security of communications has been conventionally addressed in the data link layers through scrambling and data encryption schemes. These schemes however do not secure the air interface parameters such as modulation scheme and leave them susceptible to eavesdropping and interception by man-in-the-middle platforms. Physical layer security schemes such as directional modulation, DFT S OFDM and RF fingerprinting have been proposed. In this paper, we propose a novel physical layer encryption scheme based on the spectral profile of the intended modulated signal through deliberately introduced constellation distortion to conceal the modulation scheme. The scheme uses a dispersive filter in the modulator with unique group delay profiles unknown to the eavesdropper. The appropriate inverse filter is employed in the authorized receivers to recover the original modulated basebands for demodulation.**

Keywords—Physical Layer Security.

I. INTRODUCTION

Modern wireless communication systems such as 5G and Next Generation High Throughput Satellite networks employ wideband vector modulated carriers having bandwidths over 60 MHz per channel to communicate the data of interest between the nodes in the network. Security of communications is conventionally handled in the upper layers of the network stack with techniques such as scrambling and data encryption. These techniques however do no protect the air interface of the wireless network and therefore leave the nodes susceptible to eavesdropping by man-in-the-middle interceptors [1,2]. Physical layer security schemes such as directional modulation, RF fingerprinting, Discrete Fourier Transform Spread Orthogonal Frequency Division Multiplexing (DFT-S-OFDM) have been proposed in [3, 4, and 5]. [1,6] explain schemes for secure generation of shared encryption keys based on the quasi-static and reciprocal nature of the wireless communication channel between any two authorized nodes in a wireless network. A physical layer security scheme based on fast hopping of polarizations in a satellite network is proposed in [9].

The hardware involved in the generation of a wideband modulated signal itself often requires calibration to mitigate the bandwidth specific impairments such as wideband ripple, tilt and non-linear group delay variation which in combination can introduce distortion in the constellation of the modulated signal.

In this paper we propose a novel scheme to encrypt the physical layer by exploiting the parameter Group Delay (GD) to secure the physical layer and complement the published physical layer security schemes.

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 GD variation across the occupied bandwidth and its inverse operation at the authorized receiver to recover the original modulated signal. The experimentally measured results to validate the technique are presented in section III. Finally in section IV we cover the main conclusions from this work.

II. THE PROPOSED SCHEME

The generalized block diagram of a wireless transmitter is shown in Fig **1**. 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 the applied to 'Digital to Analogue converters' (DACs) whose outputs are vector up-converted to the intended RF carrier frequency, amplified and transmitted.

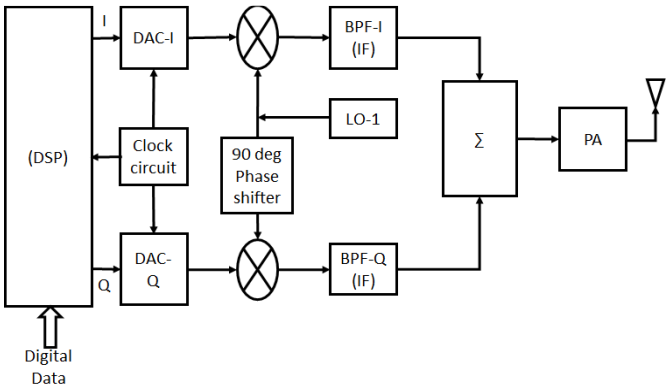

Fig 1: Generalized Block diagram of a wireless transmitter

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. As described in section 'I', the encryption in the upper layers do not conceal the air-interface. One of the ways to reduce the probability of interception is to conceal the modulation parameters of the transmitted carrier by introducing a known amount of distortion in the constellation generated by means of a secret key known only to the authorized nodes. It is assumed that the generation and agreement of physical layer dependent key described in [1, 6] have been successful.

One of the key parameters of the physical layer components that can have an adverse impact on the integrity of the modulation 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.

$$\boldsymbol{GD = \frac{d\theta}{d\omega}} \qquad (\mathbf{1})$$

Where GD is the group delay in seconds, θ is the phase in radians and ω is the angular frequency in radians/second. It's a parameter that refers to the dispersion of the individual frequency components that constitute the spectrum of the desired modulated signal. This is a key parameter to be considered in the selection of RF front end filters.

The modulation symbol generation, wave shaping and baseband filtering operations are handled by a DSP in most modern wireless communication equipment. 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 in a Hamming window based truncated Sinc filter whose impulse response is defined by the kernel:

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

Where *fc* 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 frequency response of this filter is as shown in Fig 2.

Linear phase response in the band of interest would imply a constant GD. This could be verified mathematically by taking the first derivative of a straight line which would yield a constant equal to its slope. This refers to a non-dispersive transfer characteristic of the filter. This filter may be made dispersive enough to cause constellation distortion if ripples of suitable amplitudes are introduced in the phase response of the filter thereby making GD and its variation non-linear. Experimental results in [7] 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 Ts is introduced.

This paper 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).

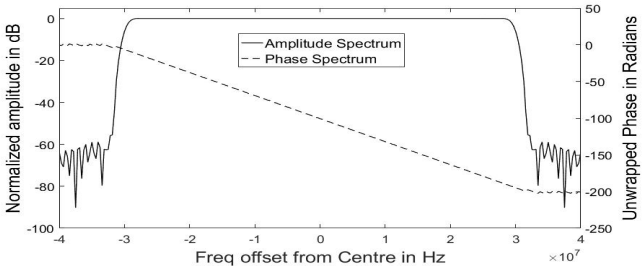

Fig 2 Spectral characteristics of a digital FIR fiilter.

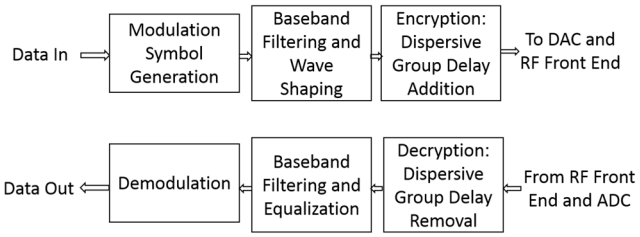

Fig 3 Proposed Physical Layer Encryption Scheme

It is proposed to exploit this impairment to our advantage in securing the physical layer by concealing the modulation scheme with the use of a dispersive filter of known GD profile at the transmitter and its inverse at the authorized receiver to recover the original modulated signal as depicted in Fig 3. The exact profile of GD variation used in the transmitter needs to be known to the receiver to undo the distortion caused and recover the original modulated signal and demodulate it.

The proposed scheme of securing the physical layer by encryption of the modulation constellation in the transmitter and decrypting it in the receiver are described in the following steps.

i) Obtain the symbol rate, occupied bandwidth (BW) and modulation constellation of the modulated carrier intended to be transmitted.

ii) Calculate the minimum variation in GD over the bandwidth of interest needed to cause constellation distortion using the mathematical relation:

$$\boldsymbol{\frac{GD}{Ts} \geq 1.15} \qquad (\mathbf{3})$$

iii) Calculate the peak variation $d\theta_{max}$ required in the phase response by equating $d\omega$ in equation '1' to BW noted in step 'i' and using the value of GD obtained in step 'ii'.

iv) Design an FIR filter kernel for the intended i.e. occupied bandwidth of the modulated signal using the kernel defined in equation '2'.

v) Obtain the Fast Fourier Transform (FFT) of the filter designed in step 'iv', extract the amplitude and phase values of the resulting spectrum.

vi) 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 35 MHz, generated digitally at a sample rate of 160 MHz and if the number of points chosen for FFT is 512, the number of FFT points occupied by the signal of interest would be 128. Since FFT is a 2 sided spectrum, half of the frequency components of would occupy the position from 1 to 56 and the other half would occupy the points 457 to 512 in the example considered.

vii) Design a non-linear curve having a peak value equal to the peak phase deviation $d\theta max$ obtained in step 'ii' with a period equal to or lesser than half of the number of points occupied by the bandwidth of interest i.e. 56 in the above example. For example, consider a sinusoidal phase variation of peak value $d\theta max$ and period 56 points. This could be designed in the form of a sine or a cosine curve. The individual values in the curve thus designed represent the phase offsets or deviations from a linear phase profile at each frequency component in the band of interest. For example,

$$\mathbf{d\theta(n) = d\theta_{max}.\cos\left(\frac{2\pi n}{56}\right)} \qquad (4)$$

Where n ranges from 1 to 56, $d\theta(n)$ is the phase offset at FFT point 'n'. Cosine function could be replaced by a phase randomization function for OFDM carriers to further reduce the probability of intercept by eavesdroppers.

viii) Add the phase offsets generated in step 'vii' to the phase components of the FFT obtained in step 'v' in the band of interest i.e. FFT point numbers 1 to 56 and 457 to 512 in the above example.

ix) Now, obtain the Inverse Fast Fourier Transform (IFFT) of the modified FFT in step 'viii'. This yields a kernel for a dispersive filter which could be convolved with the modulated baseband intended to be transmitted to conceal its modulation parameters.

x) Invert the phase components of the modified FFT obtained in step 'viii' and obtain its IFFT. This yields the kernel for the recovery filter to be used in the receiver to undo the distortion caused in step 'ix' and recover the modulated baseband.

xi) The initial phase of the function in equation 4 may be shifted at predetermined intervals in accordance with a pre-determined and agreed pseudo random hop sequence generated using the location of the nodes and RF fingerprinting techniques described in [1,4 and 6].

III. Experimental Validation.

An 8PSK signal was generated in accordance with DVB-S2 standard at a symbol rate of 40 Msps, shaped with a Root Raised Cosine (RRC) filter of roll off factor 'α' of 0.2 resulting in an occupied bandwidth of 48 MHz. A dispersive filter was designed in MATLAB as described in equation 4 with a peak phase deviation of 10 radians. This filter was convolved with the 8PSK signal to cause constellation distortion to conceal the modulation scheme. The in-phase and quadrature parts of the resulting baseband signal were quantized and applied respectively to channels 1 and 2 of DAC 34SH84 of Texas Instruments to generate the analogue equivalent baseband signals. These analogue baseband signals were vector up-converted to Ku Band at a carrier frequency of 14.23 GHz. The RF front end including the DACs and the Ku Band up-converter were calibrated to mitigate the effects of parasitic amplitude ripple and tilt, group delay and IQ imbalance over the band of interest [8]. The constellation of the modulated Ku Band carrier was observed on a Vector Signal Analyzer (VSA) 'FSQ' of Rohde and Schwarz which was used as a reference receiver.

i) Undistorted condition: This was the modulated signal constellation before application of the proposed encryption scheme. The screenshot of the 8PSK constellation demodulated by the VSA is shown in Fig 4. The Error Vector Magnitude (EVM) displayed by the instrument was 4.8%.

ii) Encrypted/Distorted condition: This was the condition after the proposed physical layer encryption scheme was applied. The constellation could not be identified as shown in Fig 5.

iii) Decrypted/Recovered Condition: This was the condition after applying the recovery filtering to the signal encrypted in 'ii'. The screenshot of the 8PSK constellation demodulated by the VSA is shown in Fig 6. The Error Vector Magnitude (EVM) displayed by the instrument was 4.9%. This

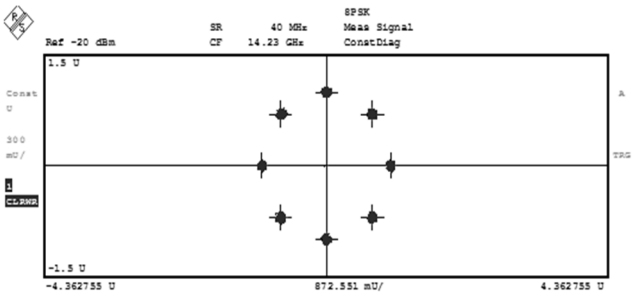

Fig 4. Demodulated constellation of the original 8PSK signal captured on R&S FSQ at 14.23 GHz

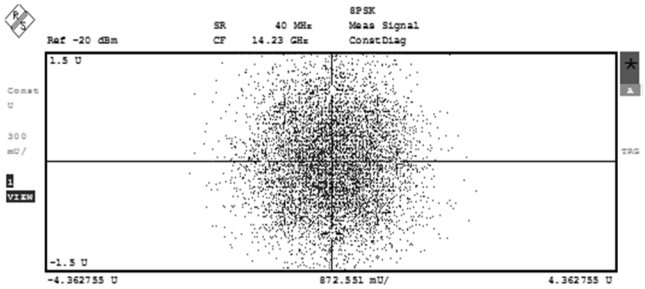

Fig 5. Demodulated constellation of the physical layer encrypted 8PSK signal captured on R&S FSQ at 14.23 GHz

was done to verify that the encryption process could be reversed.

No change was observed in the power spectrum or occupied bandwidth in all the above cases as shown in the spectrum comparison screenshot shown in Fig 7. The spectrum plots are nearly indistinguishable.

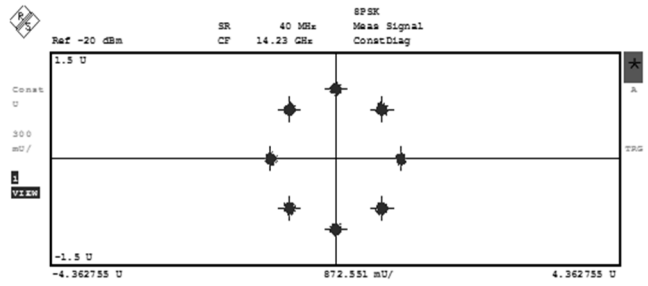

Fig 6. Demodulated constellation of the physical layer decrypted 8PSK signal captured on R&S FSQ at 14.23 GHz

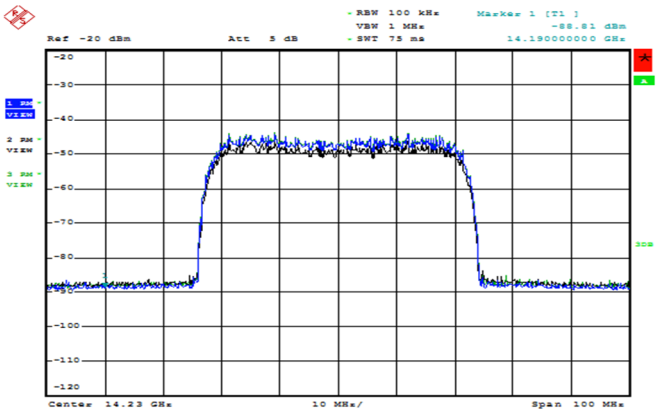

Fig 7. Power spectrum comparison screenshot captured on R&S FSQ at 14.23 GHz. Trace 1 (black): Original 8PSK carrier, Trace 2 (blue): Encrypted 8PSK carrier, Trace 3 (green): Decrypted 8PSK carrier

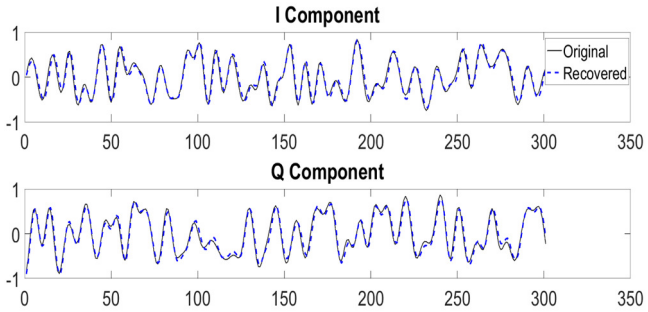

Fig. 8 Comparison of the demodulated baseband I and Q waveforms from the original carrier and from the encrypted carrier after recovery with the decryption filter.

The internal vector demodulator of the VSA was used to capture the demodulated vector 'I-Q' basebands of the original unmodified carrier and the encrypted carrier. The captured 'I-Q' basebands were imported into MATLAB. The demodulated IQ basebands of the encrypted carrier were subject to recovery filtering and compared with the demodulated 'I-Q' basebands captured for the unmodified carrier and they indicated a close match as seen in the plots of Fig. 8

IV Conclusion

The proposed technique provides a low complexity viable scheme of encrypting the physical layer in wireless communication equipment. The scheme requires no additional RF power or bandwidth. The scheme can be used alongside any of the existing published physical layer security techniques to complement their capabilities and the scope can be expanded to MIMO and carrier aggregated communication schemes with ease.

References

[1] B. Z. Katz, C. Sahin and K. R. Dandekar, "Real-time wireless physical layer encryption," 2016 IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON), Clearwater, FL, 2016, pp. 1-4. doi: 10.1109/WAMICON.2016.7483851.

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

[3] Y. Ding and V. Fusco, "Improved physical layer secure wireless communications using a directional modulation enhanced retrodirective array," 2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS), Beijing, 2014, pp. 1-4.doi: 10.1109/URSIGASS.2014.6929294.

[4] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang and H. H. Chen, "Physical layer security in wireless networks: a tutorial," in IEEE Wireless Communications, vol. 18, no. 2, pp. 66-74, April 2011. doi: 10.1109/MWC.2011.5751298.

[5] Gao Baojian, Luo Yongling, Hou Aiqin, Zhao Xiaoning and Wu Qian, "New physical layer encryption algorithm based on DFT-S-OFDM system," Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), Shengyang, 2013, pp. 2018-2022. doi: 10.1109/MEC.2013.6885382.

[6] C. Sahin, B. Katz and K. R. Dandekar, "Secure and robust symmetric key generation using physical layer techniques under various wireless environments," 2016 IEEE Radio and Wireless Symposium (RWS), Austin, TX, 2016, pp. 211-214. doi: 10.1109/RWS.2016.7444407

[7] A. Azizzadeh and L. Mohammadi, "Degradation of BER by Group Delay in Digital Phase Modulation," 2008 Fourth Advanced International Conference on Telecommunications, Athens, 2008, pp. 350-354. doi: 10.1109/AICT.2008.31

[8] Prasidh Ramabadran, Sidath Madhuwantha, Pavel Afanasyev, Ronan Farrell, Lazaro Marco, Sergio Pires and John Dooley, "Digitally Assisted Wideband Compensation of Parallel RF Signal Paths in a Transmitter" 91st ARFTG conference, Philadelphia, USA, 2018 DOI: 10.1109/ARFTG.2018.8423839.

[9] X. Zhang, B. Zhang and D. Guo, "Physical Layer Secure Transmission Based on Fast Dual Polarization Hopping in Fixed Satellite Communication," in IEEE Access, vol. 5, pp. 11782-11790, 2017. doi: 10.1109/ACCESS.2017.2710081