

Secure Wireless Communications Based On Antenna Array Elements

Shaddrack Yaw Nusenu

Koforidua Technical University, Koforidua, Ghana, Faculty of Engineering.

Abstract

Configuration of antenna array system to offer directional dependent modulation has the capability of enhancing the security level of data transmission against eavesdroppers' attacks. In this paper, Frequency diverse array (FDA) antenna for physical-layer security in wireless communications has been proposed. The proposed method provide a range and angle dependent directional modulation scheme using FDA with frequency increments to improve physical-layer security point-to-point communications. It maintains the objective of changing the progressive phase shifts at each symbol transmission. Thus the emitted pattern at each symbol transmission period will be range and angle dependent. Consequently, the proposed method offers a robust physical-layer security for wireless transmission, as the transmitted signal will be deliberately distorted along the undesired positions, but can be successfully decoded by the intended receiver position. Numerical results are presented to validate the effectiveness of the proposed method.

Keywords: Frequency diverse array; Physical-layer security; Directional antenna modulation; Wireless communication; Range and angle dependent.

1. Introduction

In recent years, the use of mobile phones, multimedia applications and internet has increased rapidly. These applications exploits the wireless links to send sensitive data being communicated in the wireless channel. The future of communication systems is expected to be decentralized and ad-hoc, enabling different types of networks terminals to be connected and disconnected (Marco Di Renzo et al. 2009). Due to the broadcast nature of wireless communication transmissions, any user within the communication directions of the intended receiver can eavesdrop the useful information. Generally the wireless communication networks adopts the open systems interconnection (OSI) protocol architecture, namely application layer, transport layer, network layer, medium access control layer and physical layer (M. M. Rashid et al. (2009), F. Foukalas et al. (2008), R. Jurdak et al. (2004), M, Takai et al. (2001) and C. Saradhi et al. (2009). Conventionally, security technique, such as cryptography was adopted to provide encryption, authentication, confidentiality and so on, at protocol stack level. However, this cryptography technique requires extra computational power and might not work efficiently in the wireless

complex environment (Yulong Zou at al. 2016). Fig. 1 shows the wireless security design approach and this design approach should be addressed and balanced in wireless complex environment.

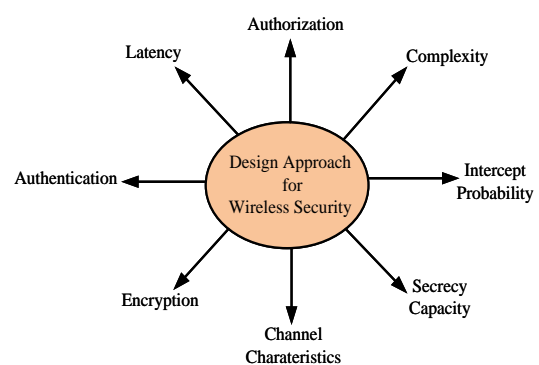


Fig.1: Illustration of design approach for wireless security (Yulong Zou et al. 2016).

In the conventional wireless communication transmitter, the transmitted information is modulated at the baseband level and up-converted to radio frequency (RF). This modulated RF signals is amplified by the power amplifier and then fed to the

antenna array. It is important to note that at the sidelobe of the transmit antenna emits the same information from this conventional transmitter. Thus, a receiver located at the transmit antenna’s main beam and that of the sidelobe, receives the same information at different locations but different signal power. If eavesdropper with sophisticated receiver is located along the sidelobe direction then the useful information can easily be intercepted. The scenarios is depicted in Fig. 2.

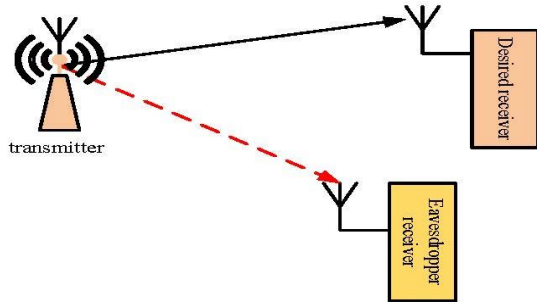


Fig.2: Illustration of a conventional wireless communications in the presence of an eavesdropper attack.

Recently, physical-layer security has attracted a lot of attention (Y. Hwang et al. (2994), Y.-S. Shiu et al. (2011) and M. Bloch et al. (2011). In physical layer protocol stack, the main security threats are shown in Table 1a.

Table 1a

Wireless security threats at Physical-layer.

Security threats	Threats Activities
Eavesdropping	Interception of confidential data
Jamming	Disruption of legitimate transmission

In this paper, a solution is proposed to prevent eavesdroppers’ threats in range and angle position. Physical-layer exploits the unique channel characteristics in order to prevent the eavesdroppers from successfully demodulating useful information intended for the desired receiver. The main goal of physical-layer security is to provide low probability of interception (LPI) and low probability of detection (LPD).

Directional antenna modulation (DAM) which has been recently proposed offers a means for achieving this (A. Babakhani et al. (2008) and A. Babakhani et al. (2009).

The basic concept of DAM is that the baseband modulation is fed to the carrier frequency to be up-converted. The radiation pattern of the transmit antenna is modified as a result of the carrier signal, thus introduces extra degree of complexity making eavesdropper task difficult. M. P. Daly et al. (2009) and M. P. Daly et al. (2010) proposed a similar concept called directional modulation (DM) to improve the security of wireless communication systems. The proposed DM technique employs phased-array antenna to prevent the eavesdroppers from intercepting the same useful information that are radiated from the sidelobes.

DAM technique has the capability to provide a secure wireless communications, since it transmits a signal with a known modulation format to the desired receiver along the pre-specified direction. The transmitted signal can be successfully recovered by the desired receiver with a prior knowledge of the modulation format. The most important attribute of DAM technique that at any distinct directions from the desired direction, the modulation format imposed on the transmitted signal changes (H. Shi et al. 2013 and Hong Zhe Shi (2014).

On the hand, Antonik (2009) proposed a flexible beam scanning array called frequency diverse array (FDA). It is important to note that the FDA can also be used for wireless communication to provide secure data transmission (Y. Ding (2015). The most important difference between FDA and phased-array antenna is the small frequency increments used across the array elements. The beam pattern changes as a function of the range, angle and time (W.-Q. Wang (2015) and P. F. Sammartino (2013) due to the frequency increments.

Therefore, this paper, proposes a range and angle dependent DAM scheme using FDA with linearly increasing frequency increments for secure point-to-point wireless communications.

The remainder of this paper is organized as follows: Section II proposed methodology structure is provided. Section III, describes the simulations and results while Section IV concludes the paper.

2. Methodology

In this section, the main contributions can be summarizes as:

- (1) FDA antenna elements are employed to achieve directional range-angle dependent for 4-ary and 8-ary transmission.

(2) The signal constellations are controlled by the linearly frequency increments of the FDA antenna elements. In such a fashion, signal-to-noise ratio (SNR) of the signals arriving at the undesired positions can be significantly reduced without SNR reduction for the desired receiver.

(3) The phased-array DAM is extended to FDA DAM and a systematic pattern synthesis procedure is presented for secure point-to-point communications. It achieves secure communications at both range and angle dimensions, not just at angle dimension as phased-array-based DAM methods.

2.1 FDA Range-Angle Dependent Transmit Beampattern

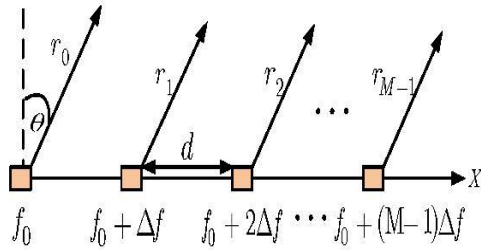


Fig. 3: Standard FDA array antenna structure.

FDA array antenna is shown in Fig. 3. The narrow-band monochromatic signal emitted from each element is identical but with a frequency increment Δf . The radiation frequency of the m th element can be expressed as

$$f_m = f_0 + m\Delta f, \quad m = 0, 1, \dots, M-1. \quad (1)$$

where f_0 is the carrier frequency and M is the number of antenna elements. The signal transmitted by the antenna element can be expressed as

$$s_m(t) = \exp(-j2\pi f_m t) \quad (2)$$

The far-field point (r, θ) signal arrival can be given as

$$s_m\left(t - \frac{r_m}{c_0}\right) = \exp\left\{-j2\pi f_m\left(t - \frac{r_m}{c_0}\right)\right\} \quad (3)$$

where c_0 is defined as the speed of light, d is the distance between the elements and the slant range for the m th array element is given in (4).

$$r_m \approx r - md \sin \theta \quad (4)$$

Accordingly, the array factor (AF) can be expressed below (P. F. Sammartino (2013) when uniform weights is considered.

$$AF(t, r, \theta) = \sum_{m=0}^{M-1} \exp\left\{-j2\pi f_m\left(t - \frac{r_m}{c_0}\right)\right\} \approx e^{-j\Phi_0 \beta} \quad (5)$$

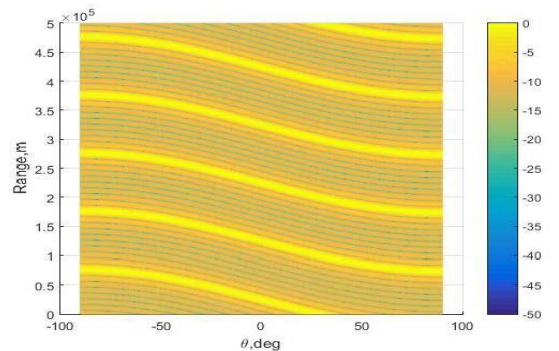
where

$$\Phi_0 = 2\pi f_0\left(t - \frac{r}{c_0}\right) - \pi(M-1)\frac{\Delta f r}{c_0} + \pi(M-1)\frac{d f_0 \sin \theta}{c_0} + \pi(M-1)\frac{d \Delta f \sin \theta}{c_0}$$

and

$$\beta = \frac{\sin\left[M\pi\left(\Delta f t - \frac{\Delta f r}{c_0} + \frac{d f_0 \sin \theta}{c_0} + \frac{d \Delta f \sin \theta}{c_0}\right)\right]}{\sin\left[\pi\left(\Delta f t - \frac{\Delta f r}{c_0} + \frac{d f_0 \sin \theta}{c_0} + \frac{d \Delta f \sin \theta}{c_0}\right)\right]}$$

Equation (5) shows that FDA transmit beampattern depends on range, angle and time. It is worth mentioning that if $\Delta f = 0$, conventional phased-array antenna is obtained and it is angular dependent only. The transmit beampatterns for FDA and conventional phased-array is shown in Fig.4. It can be noticed that in Fig. 4(a) the beampattern for FDA is range and angle dependent. In contrast, Fig. 4(b) shows the phased array antenna with its beampattern being only angle dependent.



(a)

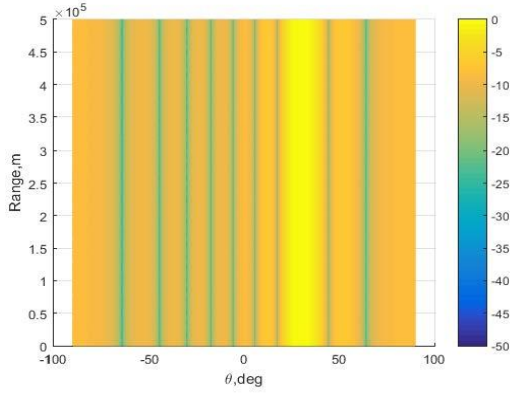


Fig. 4: Comparisons of transmit beam pattern when the array is steered to $\theta = 30^\circ$ and $\Delta f = 3 \text{ kHz}$ (a) Standard FDA. (b) Conventional Phased-array.

2.2 FDA-Based DAM for Secure Point-to-Point Wireless Communications.

Fig. 5 shows the FDA-based DAM transmitter configuration for 4-ary and 8-ary transmission. The signals are modulated directly by changing the phase pairs at the antenna level to produce directional dependent signal transmission. By properly designing the phase pairs for the FDA antenna elements, a desired constellation pattern can be generated. This signal constellation can be successfully demodulated at the specified desired range and angle position. And simultaneously distorting radiated constellations significantly along other undesired positions.

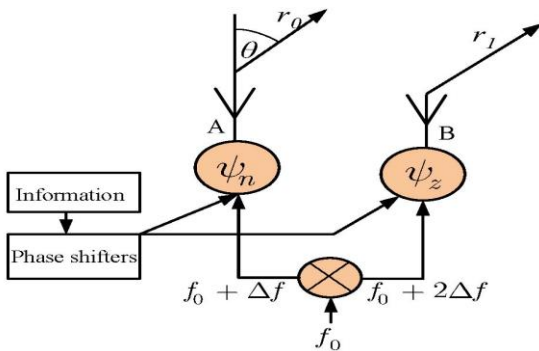


Fig. 5: Illustration of proposed FDA based DAM transmitter.

By applying DAM technique, the corresponding FDA array factor can be expressed as

$$AF(\theta, r) = \sum_{m=1}^M e^{j\psi_{nz}(t)} e^{-j[(m-1)\frac{2\pi}{\lambda}d\sin\theta - \frac{2\pi\Delta fr}{c_0}]}$$

(6)

Where $e^{j\psi_{nz}}$ is defined as the time-dependent phase. According to the proposed FDA-based DAM transmitter shown in Fig. 5, the transmitted signals can be written as in (7)

$$s(\theta, r) = e^{j\psi_n(t)} + e^{-j[\psi_z(t) - \pi \sin\theta - \frac{2\pi\Delta fr}{c_0}]}$$

(7)

where $e^{j\psi_n}$ and $e^{j\psi_z}$ represents the phase pairs of the elements, respectively. The frequency increment Δf value can be fixed or adjusted when considering different signal transmissions. The phase pairs provided by the FDA transmitter are based on assumptions and their corresponding values are shown in Table 1b and Table 2, respectively.

Table 1b

Possible Phase Pairs for 4-ary signal transmission.

Phase Pairs in degrees	
0	90
180	90
180	-90
0	-90

Table 2

Possible Phase Pairs for 8-ary signal transmission.

Phase Pairs in degrees	
45	45
45	135
135	135
135	225
225	225
225	315
315	315
315	45

3. Results and Discussions

3.1 Directional modulated 4-ary signal transmission Analysis

Fig. 6 shows the 4-ary signal constellations when $\Delta f = 3 \text{ kHz}$ is used. The 4-ary signal constellation at the desired position $(R, \theta) = (100 \text{ km}, 0^\circ)$ can be easily demodulated by the desired receiver. However, even with the same range but different angle for undesired position $(R, \theta) = (100 \text{ km}, 60^\circ)$ as shown in Fig. 7, the 4-ary constellations received is significantly distorted. Thus making eavesdropper task difficult to decode the received signal.

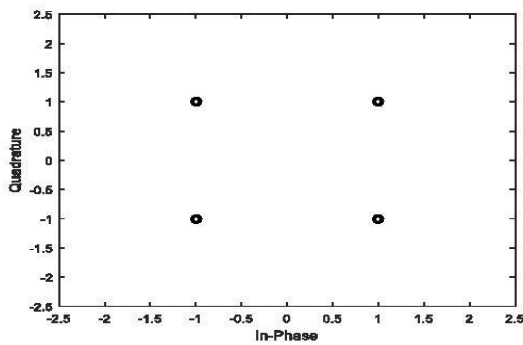


Fig.6: Illustration of proposed method 4-ary constellation pattern at intended recipient.

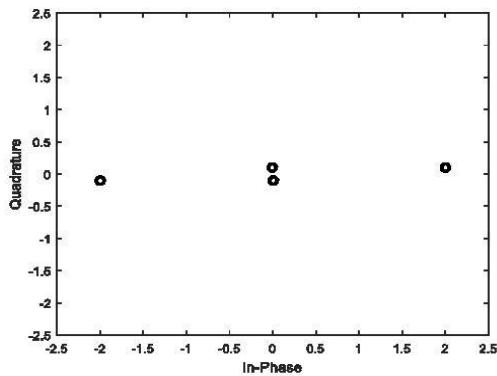


Fig.7: Illustration of proposed method 4-ary constellation pattern at other angle and range direction distorted.

Furthermore, another undesired position $(R, \theta) = (50 \text{ km}, 30^\circ)$ is examined in Fig. 8. Obviously, the received 4-ary constellations are significantly distorted. Thus, it can be concluded that the proposed method achieves corrupted constellation signals for any positions distinct from the desired range-angle position. Equivalently, it will be difficult for an eavesdropper to accurately demodulate the received signals.

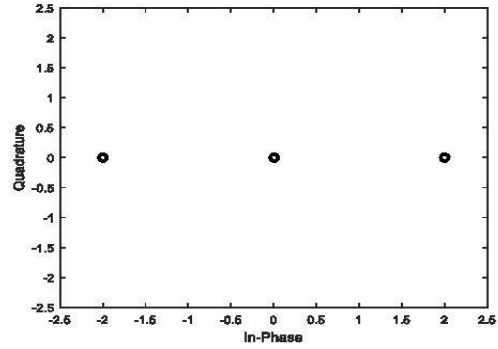


Fig.8: Illustration of proposed method 4-ary constellation pattern at other angle and range direction distorted.

3.2 Directional modulated 8-ary signal transmission Analysis

When 8-ary transmission is considered, Fig. 9 shows the 8-ary signal constellation at the desired receiver position $(R, \theta) = (100 \text{ km}, 0^\circ)$. The modulated signal can be easily decoded.

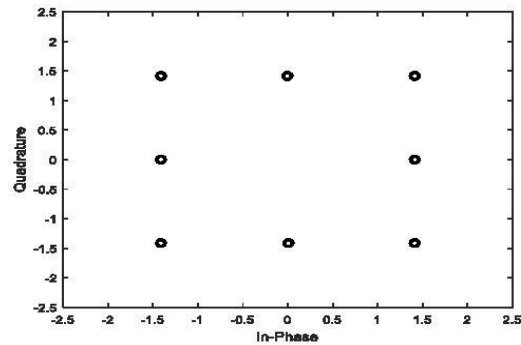


Fig.9: Illustration of proposed method 8-ary constellation pattern at intended recipient.

However, at undesired receiver position such as $(100 \text{ km}, 60^\circ)$ as shown in Fig. 10, the distorted signal constellations will make an eavesdropper task difficult to correctly decode the received signal. Similarly, another undesired receiver position such as $(50 \text{ km}, 30^\circ)$ as shown in Fig. 11 is examined. Obviously, the received 8-ary constellations are significantly distorted. Therefore, it can be concluded that the proposed method achieves corrupted constellation signals for any positions distinct from the desired range-angle position. It is important to note that the frequency increment Δf can also be exploited to improved security performance.

Finally, bit error rate (BER) performance between the proposed method and phased-array based DAM method is compared. Fig. 12 shows the BER performance in angle dimension. It can be

noticed that in angle dimension the BER characteristic achieves narrower beamwidth than the phased-array method. Thus the proposed method outperform the phased-array based method. However, in range dimension as shown in Fig. 13, the phased-array based method lacks range resolution capability. In contrast, the proposed method achieves significant BER performance in the range dimension as a result of frequency increment Δf . These results confirms that, the proposed method has good security performance in both range and angle dimensions, not in angle dimension as the phased-array based method.

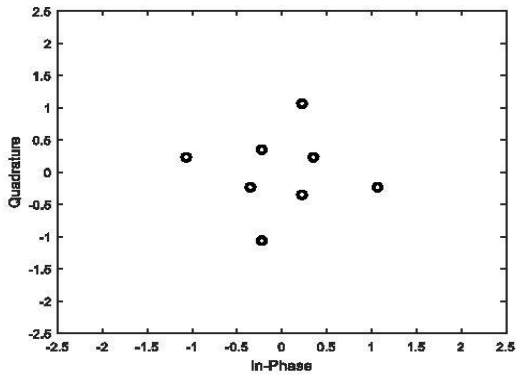


Fig.10: Illustration of proposed method 8-ary constellation pattern at other angle and range direction distorted.

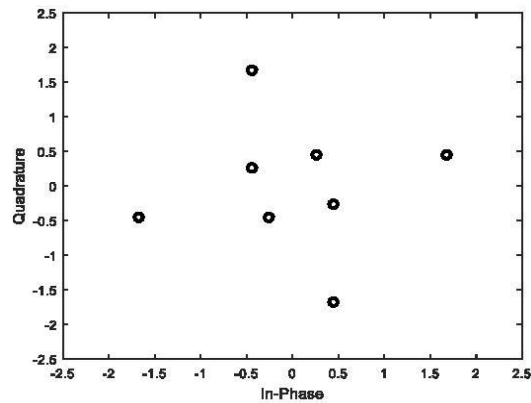


Fig.11: Illustration of proposed method 8-ary constellation pattern at other angle and range direction distorted.

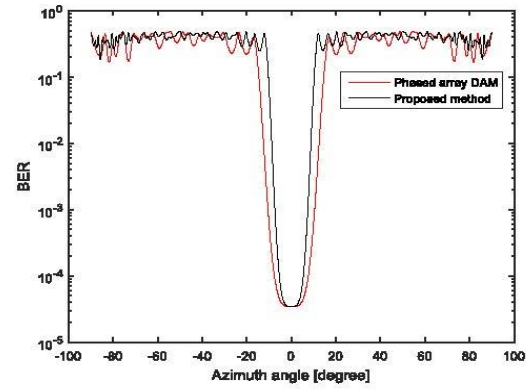


Fig.12: BER performance in angle dimension.

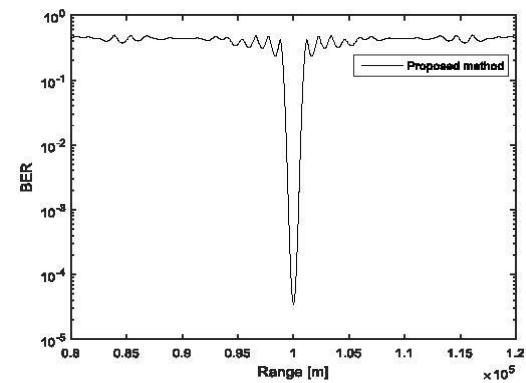


Fig. 13: BER performance in range dimension.

4. Conclusion

The proposed method takes the advantages of direct antenna modulation scheme and FDA to improve physical-layer security. The proposed FDA-based DAM method using FDA antenna achieves both range and angle dependent DAM for secure 4-ary and 8-ary wireless communications. Unlike the conventional phased-array-based DAM method, which scrambles the desired constellations only in undesired angles, the proposed method scrambles the signal constellation in both range and angle dimensions. The transmitted signals can be recovered successfully from the pre-specified range-angle position. This implies that the proposed method has the characteristics of low probability of interception (LPI) which is useful for physical-layer secure communications. Although point-to-point communications is considered in this paper, it is necessary to note that the proposed method may be also feasible for LPI radar applications.

References

- A. Babakhani, D. B. Rutledge and A. Hajimiri (2008). Transmitter architectures based on near-field direct antenna modulation. *IEEE Journal Solid State Circuits*, vol. 43, no. 12, pp. 2674–2692.
- A. Babakhani, D. Rutledge and A. Hajimiri (2009). Near-field direct antenna modulation. *IEEE Microwave Magazine* vol.10, no.1, pp.36–46.
- C. Saradhi and S. Subramaniam (2009). Physical layer impairment aware routing (PLIAR) in WDM optical networks: Issues and challenges. *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 109-130.
- F. Foukalas, V. Gazis, N. Alonistioti (2008). Cross-layer design proposals for wireless mobile networks: A survey and taxonomy,” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 1, pp. 70-85.
- Hong Zhe Shi (2014). Physical layer communication using direction antenna modulation. *PhD. dissertation, University Sheffield, London*.
- H. Shi and A. Tennant (2013). Enhancing the security of communication via directly modulated antenna arrays. *IET Microwave Antennas Propagation*. vol. 7, no. 8, pp. 606–611.
- Marco Di Renzo and M’erouane Debbah (2009). Wireless Physical-Layer Security: The Challenges Ahead. *International Conference on Advanced Technologies for Communications* pp. 313 – 316.M.
- M. Rashid, E. Hossain, and V. K. Bhargava (2009). Cross-layer analysis of downlink V-BLAST MIMO transmission exploiting multiuser diversity. *IEEE Transactions on Wireless Communications*, vol. 8, no. 9, pp. 4568-4579.
- M, Takai, J, Martin, and R. Bagrodia (2001), “Effects of wireless physical layer modeling in mobile ad hoc networks,” *Proceedings of the 2nd ACM International Symposium on Mobile ad Hoc Networking & Computing (MobiHoc)*, Carlifonia, USA.
- M. Bloch and J. Barros (2011). Physical-Layer Security from Information Theory to Security Engineering. *Cambridge, U.K.: Cambridge Univ. Press*.
- M. P. Daly and J. T. Bernhard (2009). Directional modulation technique for phased arrays. *IEEE Transactions Antennas Propagation*. vol. 57, no. 9, pp. 2633–2640.
- M. P. Daly, E. L. Daly, and J. T. Bernhard (2010). Demonstration of directional modulation using a phased array. *IEEE Transactions Antennas Propagation*. vol. 58, no. 5, pp. 1545–1550.
- Paul Antonik (2009). An investigation of a frequency diverse array,” *Ph.D. dissertation, University College London*.
- P. F. Sammartino, C. J. Baker, and H. D. Griffiths (2013). Frequency diverse MIMO techniques for radar,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 1, pp. 201-222.
- R. Jurdak, C. Lopes, and P. Baldi (2004). A survey, classification and comparative analysis of medium access control protocols for ad hoc networks. *IEEE Communications Surveys & Tutorials*, vol. 6, no. 1, pp. 2-16.
- W.-Q. Wang (2015). Frequency diverse array antenna: New opportunities. *IEEE Antennas and Propagation Magazine*, vol. 57, no. 2, pp. 145–152.
- Y. Ding, J. Zhang, and V. Fusco (2015). Frequency diverse array OFDM transmitter for secure wireless communication. *Electronics Letters*, vol. 51, no. 17, pp. 1374–1376.
- Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends, *Proceedings of The IEEE (Accepted To Appear)*, pp. 1-36.
- Y. Hwang and H. C. Papadopoulos (2004). Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: Analysis and design, *IEEE Transactions Signal Process.*, vol. 52, no.9, pp.2637–2649.
- Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S. C. Huang, and H.-H.Chen (2011). Physical-layer security in wireless networks: A tutorial, *IEEE Transactions. Wireless Communication*, vol. 18, pp. 66–74.