EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

Directional modulation techniques for secure wireless communication: a comprehensive survey

Omar Ansari[1*] and Muhammad Amin[2]

*Correspondence: omar.ansari93@yahoo.com

[1] Electrical Engineering Department, Institute of Space Technology, Islamabad, Pakistan
[2] Avionics Engineering Department, Institute of Space Technology, Islamabad, Pakistan

Abstract

Directional Modulation (DM) techniques provide wireless communication security against passive eavesdropping by means of specific physical layer characteristics. The original symbol constellations are transmitted along pre-specified spatial direction of legitimate users, while phase-amplitude distorted symbols are transmitted along the undesired directions of eavesdropper. In this paper, a comprehensive review of DM techniques and the most recent developments in this area are discussed. An analysis from three independent Physical Layer Security (PLS) viewpoints; communications, information-theoretic and cryptographic perspective is presented. Different performance metrics in literature are compared and the need for unified PLS approach is emphasized. As DM techniques constitute a relatively new class of PLS, there is no systematic organization of these techniques so far. This paper presents a classification framework for DM comprising of two main categories; angular (1D) and range-angular (2D) techniques. The former secures data along angular direction of physical space, while the latter provides security within certain range (distance) from the transmitter along desired angular direction. Further sub-categorization is based on the under-lying physical layer parameters exploited to achieve security, i.e. space, time, frequency, phase and polarization. The proposed framework is generic, flexible and extend-able to future research. In the end, limitations of existing techniques are pointed out and research directions are suggested.

Keywords: Angular directional modulation, Antenna subset modulation, Cryptography, Directional modulation techniques, Encryption strength, Frequency diverse array, Information theoretic security, Physical layer randomness, Physical layer security, Polarization sensitive array, Range-angular directional modulation, Time modulated array

1 Introduction

Wireless communication has seen unprecedented growth over the past decade. There is an ever-increasing reliance upon wireless networks for sharing confidential information, e-health, defence communication, financial transactions and banking. Seamless and secure high speed network connectivity is the demand of modern day. Extremely dense and de-centralized deployment of basestations in next generation networks is

envisioned to potentially bring about the revolutionary technological advancements of internet-of-things (IoT), machine-to-machine (M2M) and millimeter wave (mmW) short range communication. At the core of these developments, however, information security at ultra-high data rates remains a critical issue [1]. Although traditional cryptographic methods for data security are reliable and robust, their complexity and computational cost at ultra-high data rates rises exponentially. That is because these techniques rely upon bit-level operations controlled by certain highly nonlinear hard-to-invert mathematical functions. The development of light encryption algorithms focusses on lowering the computational expense by reducing the complexity of algorithm. However, light encryption algorithms are more susceptible to attacks [2].

The increasing demand for computationally cheap yet reliable data security methods have encouraged researchers to explore the lowest layer of communication protocol stack, i.e. physical (PHY) layer. Data security techniques implemented at this layer of the protocol architecture are, subsequently, called physical layer security (PLS) techniques. PLS techniques have been envisioned either to completely replace or complement existing bit-level cryptographic approaches for data security and confidentiality [3]. Another driving factor behind PLS is that 5G networks will be decentralized. If conventional cryptographic approaches are applied, key management and distribution becomes very challenging.

Directional modulation (DM) is one of the broad categories of PLS techniques that has seen a lot of research interest over the last decade. DM techniques aim to create directional information beam along a pre-specified target direction and transmit distorted signal along all the undesired directions. Hence, original constellation of data symbol is transmitted in a narrow directive beam towards the direction of legitimate user(s) only. In this way, DM techniques are effective against passive eavesdropping [4–7].

A thorough literature review suggests that there are three independent research paradigms to study PLS; communications [8–16], information-theoretic [17–21] and cryptographic treatment [22–27]. As all these paradigms are derived from independent fields of study, some stark differences between their viewpoints and performance evaluation mechanisms can be observed, as discussed in Section II. Fundamentally derived from the concepts of wireless communication, communications approach focuses on probabilistic parameters like symbol error rate (SER), mean squared error (MSE) and outage probability [11], which are directly linked to signal-to-noise ratio (SNR). Subsequently, all the optimization approaches from the perspective of communications try to maximized SNR for good signal reception for legitimate receiver while minimizing it for all the illegitimate receivers in the network. Information-theoretic approach to PLS is fundamentally structured around the idea of revolutionary Shannon's perfect secrecy systems [17]. Later on, Wyner introduced wiretap channel model [18]. It is inspired by an effort to explore the role of noise in secure communication. Secrecy capacity and secrecy outage probability are commonly used metrics for performance evaluation in this approach which are again linked to SNR [21]. Cryptographic paradigm is mostly applied on the upper layers of protocol stack. Assuming that the channel is perfectly noiseless between transmitter and receiver, channel characterization is irrelevant in this approach. This is a non-realistic assumption especially for researchers working on PHY layer for which channel noise and channel characterization are major concerns. Nonetheless,

modern encryption ciphers are designed based on this assumption of noiseless channel. Data security is measured in terms of encryption strength based on a battery of statistical randomness tests which are rigorous and extensive. Researchers from different PLS domains are beginning to notice these differences and are looking for an integrated approach for data security. Physical layer randomness (PLR) is one such metric which offers a direction comparison of encryption strength of PHY layer techniques with cryptographic encryption algorithms [22].

1.1 Existing surveys

While there are several survey papers [8–15] on PLS in general, there is only one paper specifically focussing on DM techniques [16]. In [8], authors have presented a survey of PLS and its potential for deployment in three promising wireless technologies; heterogeneous networks, massive multiple-input multiple-output (MIMO) and millimeter wave communication. The main focus of this paper is data confidentiality by techniques which use intrinsic noise of physical communication medium. A review on multiple antenna techniques for PLS is given in [9]. In this paper, transmitter beamforming designs for securing point-to-point link, multi-user system and heterogeneous networks are discussed. In [10], a survey of PLS for authentication and confidentiality by exploitation of channel randomness is presented. A survey of information-theoretic approach for data authentication and confidentiality is presented in [11]. In this paper, security techniques for MIMO, heterogeneous networks, non-orthogonal multiple access (NOMA) and PLS coding are discussed. In [12], authors have discussed security vulnerabilities and threats present in the technologies associated with 5G networks. An outline of security vulnerabilities of post-5G networks is also provided and research directions for coping with security challenges related to each technology are highlighted. A detailed survey on PLS techniques against passive eavesdropping is presented in [13]. A framework of classification is proposed which broadly classifies PLS techniques into two classes; signal-to-interference-plus-noise (SINR) based approach and complexity-based approach. In the end, recently emerging applications of PLS are highlighted. In [14], PLS research and developments are approached from an interesting viewpoint of optimization and signal processing. A detailed classification of different optimization approaches is presented. PLS techniques for satellite communication and satellite-based IoT are presented in [15]. Different architectures for security are presented and compared. Finally, a review of different DM techniques for PLS are presented in [16]. As this paper was published back in 2016, there has been major developments since that time. A summary of existing surveys and their contributions are highlighted in Table 1.

1.2 Contributions

Initially conceived in [28], DM techniques have now matured to the point of practical realization [29–31]. Data security in DM is achieved by transmitting non-encrypted data (plaintext) along a-priori known direction of intended receiver (IR) and encrypted data (ciphertext) along eavesdroppers. Ciphertext is phase-amplitude distorted version of data for which PHY layer parameters like space, time, frequency, phase and polarization can be exploited. This concise understanding has led to comprehensive classification framework of DM techniques in our paper.

Table 1 Existing surveys

Survey	Publication	Year of publication	Main focus
[8]	IEEE Communications Magazine	2015	Information-theoretic physical layer security for heterogeneous networks, massive MIMO and millimeter wave
[9]	IEEE Communications Surveys and Tutorials	2017	Multiple antenna physical layer security techniques and transmit beamforming designs
[10]	IEEE Communications Surveys and Tutorials	2017	Physical layer security technologies and challenges for next generation wireless networks
[11]	IEEE Journal on Selected Areas in Communications	2018	Information-theoretic data confidentiality for massive MIMO, millimeter wave communication, heterogeneous networks and NOMA
[12]	IEEE Communications Surveys and Tutorials	2019	Security vulnerabilities and threats in 5G and post-5G communication networks and future research directions
[13]	IEEE Communications Surveys and Tutorials	2019	Framework of classification of security techniques based on SINR and complexity-based approaches
[14]	IEEE Communications Surveys and Tutorials	2019	Optimization and signal processing techniques for physical layer security
[15]	IEEE Internet of Things Journal	2020	Physical layer security techniques for satellite based internet-of-things
[16]	International journal of microwave and wireless technologies	2016	Review of developments in directional modulation technologies
This work			Survey and classification framework of directional modulation techniques for PLS of wireless communication networks

Following are the major contributions of our paper:

(1) An updated survey focusing on the recent developments in DM for secure next generation wireless networks is presented.
(2) The analysis of DM from three different PLS viewpoints (communications, information-theory and cryptography) is presented, their differences are highlighted and the need for an integrated PLS approach is emphasized.
(3) A systematic classification framework for DM has been presented in which the primary categories are based upon the dimensional capability for security,

i.e. angular DM (one-dimensional) and range-angular DM (two-dimensional). Moreover, secondary classification is done using the underlying PHY layer parameter exploited to achieve PLS, i.e. space, time, frequency, phase and polarization. As the proposed framework is generic and flexible, future developments can benefit from it as they are very likely to fall under one or a combination of these classifications.

1.3 Organization of paper

The organization of our paper is shown in Fig. 1. An introduction is provided in Sect. 1. Section 2 outlines three different paradigms of PLS that are prevalent for the study of DM. In Sect. 3, the classification framework for DM techniques is presented and its

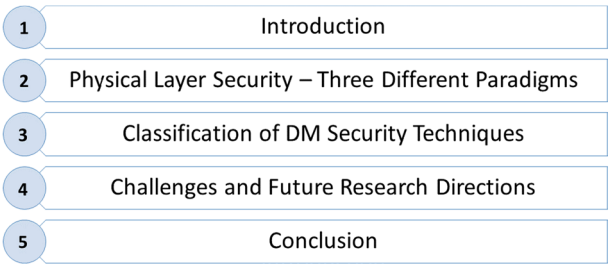

Fig. 1 Organization of the paper

relevance is discussed. Current limitations and possible research directions are pointed out in Sect. 4. The paper ends with a conclusion in Sect. 5.

2 Physical layer security—three different paradigms

There are three paradigms for studying PLS techniques; communications, information-theoretic and cryptographic paradigms. When viewed from the perspective of DM, however, each paradigm has fundamentally the same objective, i.e. transmission of information to IR and preventing eavesdropping by an adversary. Nevertheless, each paradigm has independently evolved and adopted different set of tools for analysis and evaluation of PLS as discussed in this section.

2.1 Communications paradigm

In this approach, wireless communication based tools and techniques are adopted. There are two categories of metrics which are used to measure PLS from communications paradigm: error-based and signal strength-based metrics. The most commonly used error-based parameters are bit error rate (BER), symbol error rate (SER), root mean-squared error (RMSE) and error vector magnitude (EVM). These metrics are probabilistic measure of erroneously received symbols and deviation from original transmitted symbols. Naturally, it is desirable to maintain minimum error magnitude along the direction of legitimate user and maximum error along all the undesired directions for preventing the access of information to eavesdropper. All the communications-inspired optimization approaches, therefore, aim to maximize error probability (implicitly assumed proportional to PLS) in the undesired directions while keeping its value minimum along the intended receiver. On the other hand, signal-strength based parameters such as signal-to-noise ratio (SNR), SINR and power patterns of radiating elements are maximized in the direction of legitimate user for good reception of signal, while maintaining them low in the unintended directions (Fig. 2).

In communications approach, direct concern with SNR is natural as transmitted signal is distorted by addition of channel noise and multipath effects. However, in cryptographic approach, which is mainly implemented at application layer, performance analysis is carried out assuming zero noise (infinite SNR). Another clear distinction between this approach and cryptography is that high SER does not necessarily imply strong encryption, as recently shown in [22] by analyzing DM as block encryption cipher. This result indicates contradiction between communications approach and cryptographic paradigm. This also necessitates bridging the gap between these two

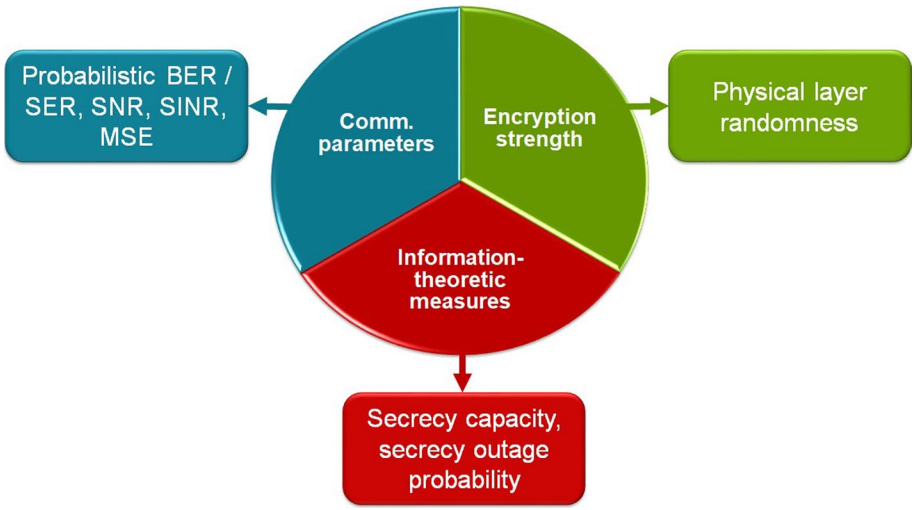

Fig. 2 Three different viewpoints (communications, information-theoretic and cryptographic encryption) from which the physical layer security of directional modulation techniques is studied are highlighted. Moreover, different parameters that are used by each approach are summarized

paradigms for an integrated PLS approach as the basic objective of all the approaches is the same, i.e. to provide communication security at physical layer.

2.2 Information-theoretic paradigm

The information-theoretic paradigm is fundamentally inspired by Shannon's perfect secrecy characterization [17] and Wyner's wiretap channel model [18]. In wiretap channel model, data encoding at transmitter and subsequent decoding at receiver are permitted. However, it is assumed that these encoding–decoding operations are known to eavesdropper as well. Moreover, information-theoretic treatment of PLS takes advantage of ubiquitous channel noise that is inherent part of the system. The physical channel from sender to eavesdropper is assumed to possess higher noise compared to the channel from sender to legitimate user, which most often is the case. The encoder is designed to maximize transmission rate for legitimate receiver, while minimizing it (ideally to zero) for eavesdropper. The idea was readily applied to secure space–time communication [32]. Later on, the analysis was extended to multi-antenna wiretap channel [33], multiple-input single-output multiple-eavesdropper (MISOME) [34], and multiple-input multiple-output multiple-eavesdropper (MIMOME) [35] scenarios with the assumption that channel matrices are fixed and known at all nodes. A generalization to arbitrary number of MIMO antennas for Gaussian wiretap channel is presented in [36]. For simplification of analysis, it is assumed that the channel states of receiver and eavesdropper are known to transmitter.

As far as DM techniques are concerned, conventional information-theoretic treatment of PLS is not directly applicable due to three major differences. Firstly, there is predominantly no encoding of information bits at DM transmitters in the known direction of receiver. Secondly, directional-modulated signals do not require decoding at legitimate receiver since plaintext is received in that direction. Finally, information-theoretic

assumption of known channel conditions at the terminals is not fulfilled. A DM transmitter only requires spatial angular and/or spatial range information of legitimate user, while the direction of eavesdropper (a passive observer in this case) remains completely unknown. These fundamental differences suggest that DM PLS is inherently dissimilar to information-theoretic PLS. Nonetheless, as the literature suggests, DM researchers have borrowed information-theoretic performance metrics, such as, secrecy capacity and secrecy outage probability for security evaluation. In communications approach, channel characteristics like SNR and SINR are directly used for quantification of communication security; while in information-theoretic analysis of DM, these parameters are indirectly used by deriving secrecy capacity and secrecy outage probability in terms of SNR and SINR.

Moreover, information-theoretic paradigm is diametrically opposed to cryptographic treatment of DM security in which more strict conditions of ideal and noiseless channel conditions are assumed. With zero channel noise, SNR is ideally infinite. This assumption violates wiretap channel approach, the very fundamental assumption of which is that the channel from sender to adversary is noisier than from sender to receiver. By assuming noiseless channel conditions, the inherent encryption strength of DM technique is quantified without the effect of any external factors like channel noise, inter-symbol interference, multi-path effects and many other realistic phenomena which are completely ignored in cryptographic treatment because they also contribute to randomness.

2.3 Cryptographic paradigm

The cryptographic paradigm of information security is based on complexity-based assumption that certain nonlinear mathematical functions are difficult to invert. Subsequently, encryption algorithms are designed using hard-to-compute mathematical operations. Symmetric-key cryptosystem is one such encryption mechanism which uses same keys both for encryption and decryption [37]. There are five main components of any modern symmetric-key cryptosystem; plaintext (P), ciphertext (C), encryption (E), decryption (D), and a set of keys (K) that are used for encryption and decryption operations. Plaintext is the original message in non-encrypted form. Ciphertext is the encrypted message obtained after applying encryption algorithm on plaintext. Decryption is the process of recovering the original message at receiver using the keys. Rivet Shamir Adelman (RSA) [38], improved data-encryption standard (DES) [39] and advanced encryption standard (AES) [40] are famous cryptosystems which are widely used for information security.

When DM techniques are analyzed from cryptographic viewpoint, certain PHY layer mappings are required [22]. Plaintext is the set of baseband symbols intended for transmission along legitimate receiver only. Ciphertext is the phase-amplitude distorted version of symbols transmitted along the direction of adversary. Encryption algorithm is the PHY layer mechanism that is used to achieve PLS. Decryption is performed by adversary in an effort to extract useful information from ciphertext. The IR does not require decryption as plaintext is transmitted in that direction. Finally, the unique set of values generated by modulation of PHY layer parameter in DM is analogous to cryptographic key.

In cryptographic analysis of DM, completely noiseless physical channel is assumed and encryption strength is evaluated by measuring randomness introduced solely by the DM mechanism. This implies that the basic parameters of other two paradigms (i.e. SNR and channel capacity) are ideally infinite. This assumption violates information-theoretic wiretap channel approach, the very fundamental assumption of which is that the channel from sender to adversary noisier than sender to receiver channel. There has been an effort to combine the two paradigms by cryptographic treatment of wiretap channel [41]. However, these paradigms remain predominantly independent. Moreover, cryptographic approach has its own unique statistical tools for evaluation of encryption strength which are more rigorous in terms of randomness evaluation and should be combined with modern PLS research. The most commonly used encryption strength evaluation tools are Statistical Test Suite (STS) [42], Dieharder battery of tests [43] and TestU01 [44].

2.3.1 Physical layer randomness

There has been an effort to unite the cryptographic paradigm with communications approach [22]. Physical Layer Randomness (PLR) is one such parameter that offers a common framework for direct comparison of encryption strength of PLS systems and cryptographic ciphers. STS is a package devised by National Institute of Standards and Technology (NIST) that is used for measuring the encryption strength of chiphertext after applying the candidate encryption algorithm [45]. It comprises of 15 standard randomness tests. Each test checks bit-level stream of data for the presence of any pattern that can render the data non-random. It is done by comparing the ciphertext with truly random sequences and probabilistic measure of randomness is evaluated in terms of p-value for each test [46]. The tests performed are; Frequency Monobits Test (FT), Block Frequency Test (BF), Runs Test (RN), Longest Runs of Ones in a Block Test (LR), Binary Matrix Rank Test (RK), Discrete Fourier Transform Test (DT), Non-Overlapping Template Matching Test (NO), Overlapping Template Matching Test (OV), Universal Statistical Test (US), Linear Complexity Test (LC), Serial Test (ST), Approximate Entropy Test (AE), Cumulative Sums Test (CS), Random Excursion Test (RE) and Random Excursion Variant Test (RV).

Based on statistical hypothesis testing, null and alternative hypotheses are formulated. Null hypothesis implies that the ciphertext is random and hence cryptographically strong. Alternative hypothesis is that the data is non-random hence susceptible to eavesdropping. Each randomness test is assigned a p-value [47] as; P_F, P_B, P_R, P_L, P_K, P_D, P_N, P_O, P_U, P_C, P_T, P_A, P_S, P_E and P_V. Based on NIST's recommendations, if p-value for any test is less than 0.01, ciphertext is weakly encrypted and alternative hypothesis is accepted. On the other hand, if p-value is greater than 0.01, null hypothesis is true and the ciphertext is strongly random. After obtaining the p-values, ranks are assigned to each p-value, as shown in Table 2. The arithmetic sum of all the ranks is defined as PLR, i.e. randomness at PHY layer. PLR serves twofold purpose; analysis of encryption strength of PHY layer techniques and its comparison with strong encryption algorithms like AES [48]. This is the only cryptographic randomness tool available today which is directly applicable to PLS techniques and provides encryption comparison with traditional cryptosystems.

Table 2 Classification of *p*-values into PLR ranks

S.No	PLR Rank	Range of p-values	Description
1	$\zeta=5$	$p-value \geq 0.5$	Extremely strongly passed
2	$\zeta=4$	$0.4 \leq p-value < 0.5$	Strongly passed
3	$\zeta=3$	$0.3 \leq p-value < 0.4$	Moderately passed
4	$\zeta=2$	$0.2 \leq p-value < 0.3$	Satisfactorily passed
5	$\zeta=1$	$0.01 \leq p-value < 0.2$	Barely passed
6	$\zeta=F$	$p-value < 0.01$	Failed

3 Classification of DM security techniques

In this section, a systematic framework for the classification of DM techniques has been presented. Based on PLS dimensional capability, these techniques can be broadly divided into two categories; angular and range-angular DM. The former provides security only along spatial angular direction, while the latter secures data with respect to both angular direction and range (distance) from transmitter. Accordingly, they can also be called one dimensional (1D) and two dimensional (2D) DM. These techniques are further classified based on the under-lying PHY layer mechanism used to achieve security. For instance, space, time and frequency are some of the commonly used PHY layer parameters. This idea is elaborated in the form of a taxonomy in Fig. 3. We will refer to this figure whenever required. Finally, PLS analysis of DM from three different security viewpoints (as discussed in Sect. 2) and application specific comparisons are provided in respective subsections.

3.1 Angular (1D) DM techniques

Angular DM techniques provide directional encryption of data only along one spatial dimension, i.e. angular direction, hence, also called 1D techniques. The non-distorted constellation of symbols (i.e. plaintext) is transmitted along pre-specified angular direction in which legitimate receiver is located. It is important to mention here that the spatial angular direction of intended receiver should be known at the transmit side before transmission. A conventional phased array transmitter is shown in Fig. 4. Alice wants to transmit a message to Bob located along an angular direction θ_{IR}. The phase shifter of each transmit branch is compensated by adjusting β to direct the main lobe in the direction of Bob. Power amplifier (PA) amplifies the signal before feeding to respective antenna for transmission. In this way, original message is transmitted along Bob's direction. An eavesdropper located outside the narrow beam of main lobe receives distorted symbols through antenna sidelobes. However, an eavesdropper can easily extract intelligible information from the transmitted data by using direction of arrival (DOA) techniques because all the symbols are distorted in a similar fashion from one symbol to another. Therefore, a typical phased array transmitter does not provide any security at PHY layer.

Depending upon the under-lying PHY layer parameter used, angular DM techniques can be classified into several sub-categories. The commonly used parameters

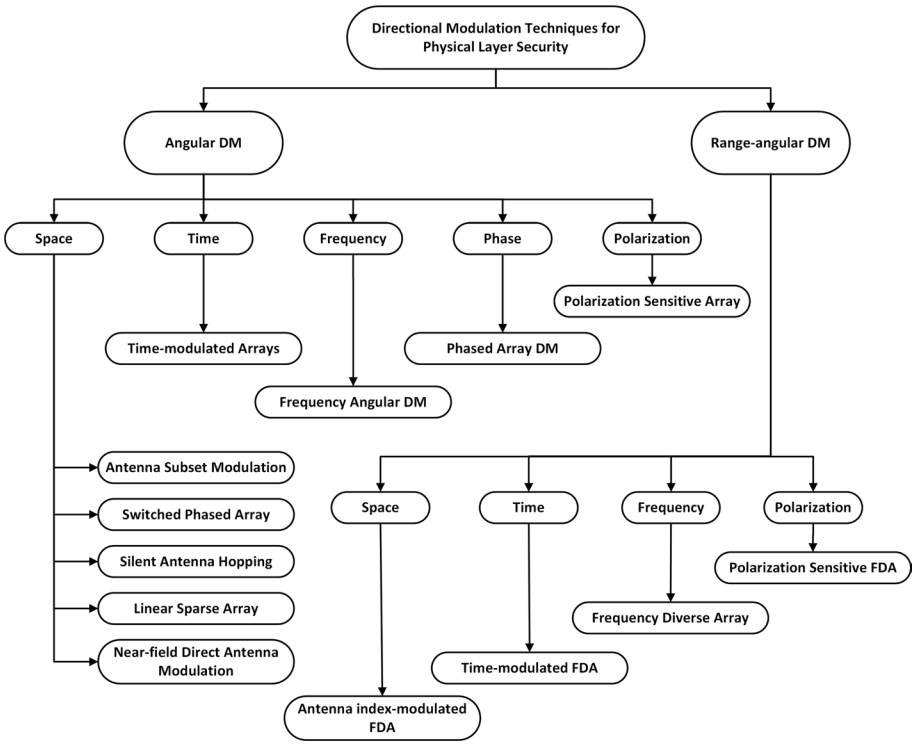

Fig. 3 Taxonomy of directional modulation techniques for physical layer security against passive eavesdropping. This figure captures the essence of the framework proposed in this paper. It categorizes directional modulation techniques into two broad categories; angular and range-angular DM. Angular DM techniques secure data only along spatial angular direction, while range-angular DM techniques transmit secure data along spatial angular direction within specified spatial range of intended receiver. The sub-categorization has been done based on the under-lying physical layer parameter used to achieve security; space, time, frequency, phase and polarization

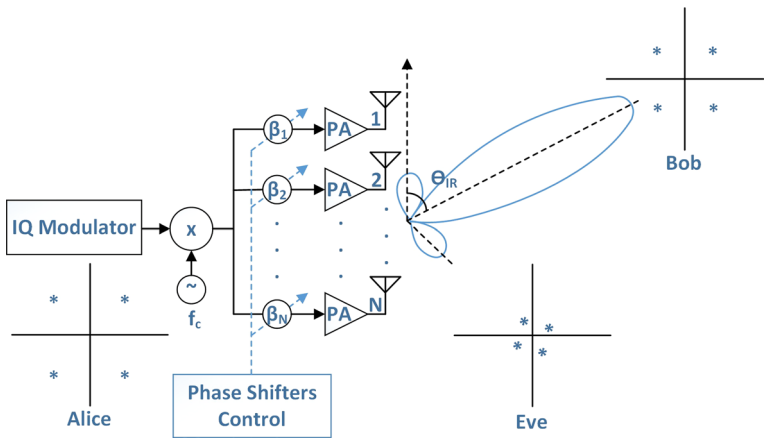

Fig. 4 The transmit architecture of a conventional phased array is shown in this figure. It is shown that conventional array transmits phase and amplitude distorted (but predictable) version of original constellation transmitted by Alice (which was intended for Bob)

in DM literature are space, time, frequency, phase and polarization. While these parameters are independently tuned to obtain the desired modulation, a combination of multiple parameters can also be used. In this section, a summary of the analysis

Table 3 Secure communication using angular directional modulation

Paper	Description	Communications parameters	Information-theoretic measures	Cryptographic strength
Spatial angular DM				
[22]	DM as block ciphers	–	–	PLR
[49]	Antenna subset modulation	SER	–	–
[50]	Antenna subset modulation	SER	Secrecy capacity	–
[51]	Low-complexity ASM	BER	Secrecy capacity	–
[52]	Eavesdropper attack on ASM	SER, SNR	–	–
[53]	Iterative FFT-based ASM	SER, beampatterns	–	–
[54]	Random ASM for vehicular networks	–	Secrecy throughput	–
[55]	Multi-antenna DM for vehicular networks	–	Secrecy rate	–
[56]	ASM as block encryption cipher	SER	–	PLR
[57]	Hamming distance maximization for ASM	–	–	PLR
[58]	Switched-antenna array for DM	BER, RMSE	–	–
[59]	Switched-phased array architecture	BER	Secrecy capacity	–
[60]	Silent antenna hopping	BER	Secrecy capacity	–
[61]	Linear sparse array based DM	SER, SLL	–	–
[62]	Convex optimization assisted LSA	BER, pattern beamwidth	–	–
[63]	Fourier network based circular array for DM	BER, power pattern	–	–
[64]	DM using retrodirective antenna array	BER, power pattern	–	–
[65]	Demonstration of 71 GHz directional PHY layer secure link	EVM, power measurements	–	–
[66]	Near-field direct antenna modulation	BER	–	–
[67]	Transmitter architecture demonstration of NFDAM	BER, data constellations	–	–
[68]	Multiple antenna array based positional modulation	BER, beam pattern	–	–
[69]	Metasurface based positional modulation	BER, beam pattern	–	–
[70]	Intelligent reflecting surfaces for multipath DM	–	Secrecy rate	–
Temporal angular DM				
[78]	Time-modulated 4D array	BER, power patterns	–	–
[79]	Hybrid DM and beamforming for 4D arrays	BER	–	–
[80]	Time-modulation based vectors for 4D array	BER	–	–
[81]	Pulse sequence optimization for TMA	Fidelity rate, BER	–	–

Table 3 (continued)

Paper	Description	Communications parameters	Information-theoretic measures	Cryptographic strength
[82]	Experimental assessment of time-modulated DM	Fidelity rate, BER	–	–
[83]	Time-modulated DM for OFDM transmitter	BER	–	–
[84]	Multi-carrier TMA	BER	–	–
Frequency angular DM				
[85]	Random sub-carrier selection for DM	SINR	Secrecy rate	–
[86]	DFT-based multi-directional DM	Power pattern	Secrecy rate	–
Phase angular DM				
[87]	Phased array based directional modulation	BER	–	–
[88]	Demonstration of phased array DM	BER, normalized pattern	–	–
[89]	Pattern-reconfigurable DM	BER	–	–
[90]	Dual-beam DM architecture	BER	–	–
[91]	Hybrid MIMO and phased array DM	BER	Secrecy capacity	–
[92]	Phased array transmitter using polygon construction	SER	–	–
Polarization angular DM				
[93]	Polarization state based PLS	SER	–	–
[94]	Crossed-dipole array based DM	SER	–	–
[95]	Directional polarization modulation	SER	–	–
[96]	Angular DM using polarization sensitive array	SER	Secrecy capacity	–

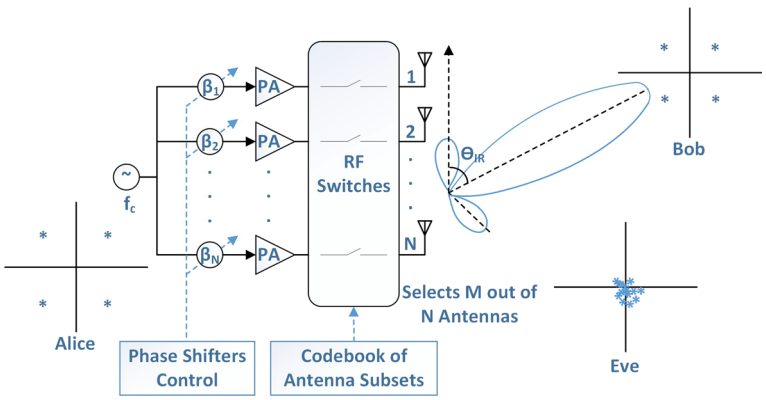

Fig. 5 Transmitter architecture of a typical angular DM for antenna subset based transmission is shown. Data constellations transmitted by Alice are correctly received in the direction of Bob. In the direction of Eve, however, constellations are distorted and randomly distributed

Table 4 Application specific comparison of angular DM techniques

S.no	Description	Applications
Spatial angular DM		
1	Switched-phased array architectures: ASM [49–51, 53–55], SPA [58, 59], SAH [60], LSA [61] [62], demonstration of 71 GHz secure link [65]	Switched-phased array DM architectures are well-suited for secure angular point-to-point wireless communication. Low-complexity and ease of implementation are two major advantages
2	Cryptography-inspired analysis of DM [22] [56], and cryptographic array optimization of ASM [57]	Focussed on cryptographic analysis and optimization of DM arrays. SLL optimization is shown to be ineffective. The need for an integrated security approach for PLS techniques is emphasized
3	Fourier network based circular array for DM [63]	It provides an added advantage of secure beamsteering along two angular directions, i.e. along elevation and azimuth, for more precise and secure transmission at the expense of increased complexity
4	DM using retrodirective antenna array [64]	Feasible for more than one user positioned along different angular directions, providing multi-directional security
5	Near-field direct antenna modulation (NFDAM) [66, 67]	Recommended for single antenna based point-to-point secure angular directional communication. Requires switching control circuitry of varactors and switches placed in the near-field of antenna
6	Multiple antenna arrays based positional modulation [68, 69]	Multiple antenna arrays positioned at different angular directions are required. Overcomes the issue of security breach in case eavesdropper is spatially close to legitimate user, but at the expense of higher complexity. Not feasible for situations in which multiple arrays cannot be placed at multiple spatial positions
7	Intelligent reflecting surfaces for multipath DM [70]	Intelligent reflecting surfaces are used to create multipath transmission. Suited for multipath DM applications
Temporal angular DM		
8	Time-modulated array for angular DM [78–82]	Antenna array is modulated with respect to sub-slots of time. Major advantage is that hardware level changes in conventional phased array transmitter architecture are not required
9	Multi-carrier TMA [83] [84]	Proposed for angular directional security of OFDM transmitter [83], and antenna level multi-carrier TMA [84]
Frequency angular DM		
10	Random sub-carrier selection for DM [85]	Secures OFDM architecture with respect to angular transmission
11	DFT-based multi-directional DM [86]	Provides multi-directional secure OFDM transmission capability
Phase angular DM		
12	Phased array transmitter [87–89, 91, 92]	Secures transmission by phase control of antenna array. Major drawback is compromised directivity due to misalignment of array phases

Table 4 (continued)

S.no	Description	Applications
13	Dual-beam phased array [90]	Uses two beams for directional transmission of data symbols. Provides better security than phased array transmitter with reduced antenna elements
Polarization Angular DM		
14	Polarization state based angular DM [93–96]	Transmission is both directionally secure and polarization sensitive. Useful for dual-polarized secure satellite applications

of angular DM techniques from three security viewpoints is presented in Table 3 and application specific comparison is provided in Table 4.

3.1.1 Spatial angular DM

In this class of DM, spatial switching is performed at antenna level. Since space is the fundamental parameter that is used to secure data along angular direction, it is called spatial angular DM. Although the basic idea behind space angular DM using switched spaced antennas dates back to as early as 1990 [30], it did not see any practical interest due to technological limitations. Over the last decade, however, there has been a lot of developments on this concept. Broadly speaking, the spatial switching can be performed either by switching the antenna itself [49–77] or by switching the elements surrounding the antenna (thus by varying the near-field electromagnetic boundary conditions). In [16], authors have classified the former as excitation-reconfigurable and latter as radiator-reconfigurable DM. This classification marks the fundamental difference between these two techniques, i.e. whether transmitter changes antenna excitation by switching antenna elements or by switching the scatterers surrounding the antenna. However, both of them still fall under the space angular DM in our classification because both techniques essentially achieve PLS by switching of spatial elements.

Antenna subset modulation (ASM) is one such DM technique that modulates randomly selected antenna subset for every symbol transmission [49]. A typical ASM transmitter architecture is shown in Fig. 5. As ASM was originally proposed for phase shift keying (PSK), the phase shifters generate not only the desired symbol's phase but also adjust inter-element phase differences. The signal is then amplified by respective PA of each branch. Before feeding the amplified power to antennas, high speed RF switches are used to select random configuration of antenna elements that is modulated at symbol rate. The resulting beamform transmit non-encrypted data along angular direction of Bob and encrypted data along the directions of eavesdropper. There are two ways in which antenna subsets can be selected; randomized antenna subset selection (RASS) and optimized antenna subset selection (OASS). The former technique randomly selects configuration of antennas, while the latter uses side-lobe level (SLL) optimized subsets. It has been shown that OASS performs better than RASS in terms of SER [50]. ASM has been analyzed from two different paradigms using the metrics of SER and secrecy capacity. A low-complexity architecture for ASM reduces its complexity by making it compatible with baseband modulation architectures [51]. In [52], a passive eavesdropper attack

is lodged on ASM. It is shown that a team of eavesdroppers situated at multiple spatial locations can make an estimate of original data. However,this approach is impractical as large number of spatially distributed eavesdroppers are required for such an attack. Iterative fast-Fourier transform (FFT) based selection of antenna subsets is shown to reduce the complexity of antenna subset selection procedure [53]. The concept of ASM for PLS has also been extended to vehicular networks for secure vehicle-to-vehicle (V2V) communication [54, 55]. The possibility of integration of large scale antenna elements onto a single chip at millimeter wave makes it practically realizable.

A recent development proposes to analyze the PLS of ASM using cryptography-inspired tools. After certain PHY layer mappings, the encryption strength of ASM has been evaluated in terms of PLR [56]. Contrary to [50], it is shown that SLL optimized OASS although performs better than RASS in terms of SER and secrecy capacity, OASS has rather adverse effects on encryption strength due to significant reduction of antenna subset combinations. Alternatively, randomness-driven approach of hamming distance maximization between successively used antenna subsets is proposed in [57]. Cryptographic PLR of hamming distance maximization has been shown to outperform SLL OASS optimization.

Switched-phased array (SPA) is another spatial angular DM [58, 59] which closely resembles ASM architecture but with two subtle differences:

(1) Unlike SPA, ASM does not use baseband modulation. The modulation of symbols is performed at passband.
(2) In ASM, fixed number of antenna elements are turned on for every symbol transmission, while SPA uses variable number of switched antenna elements.

A similar architecture of silent antenna hopping (SAH) randomly turns off only one antenna element for secure PHY layer transmission [60]. Its performance has been evaluated only from communications perspective in terms of SER. Linear sparse array (LSA) carefully optimizes array thinning ratio with respect to SLL for selection of optimum number of active antenna elements [61]. The major difference between LSA and previous switched array architectures is the number of active elements. Convex-optimization has been applied to LSA for better BER performance [62]. The concept of DM has been extended to circular arrays by using Fourier feeding network [63]. Circular DM arrays have added advantage of beamsteering in two angular directions, i.e. along elevation and azimuth. Another interesting development combines DM with retrodirective array for secure PHY layer transmission [64]. A practical demonstration of secure DM link operating at 71–76 GHz is presented in [65].

All the techniques discussed above so far were excitation-reconfigurable. On the other hand, radiator-reconfigurable space angular DM performs switching of passive elements like varactors or high speed RF switches placed around the antenna [66]. It is also called near-field direct antenna modulation (NFDAM), as the near-field electromagnetic boundary conditions are constantly changed by the high speed switching of radiators. As a consequence, PLS is achieved effectively by modulated far-field radiation pattern due to near-field switching in the vicinity of antenna. Practical realization of this architecture is presented in [67].

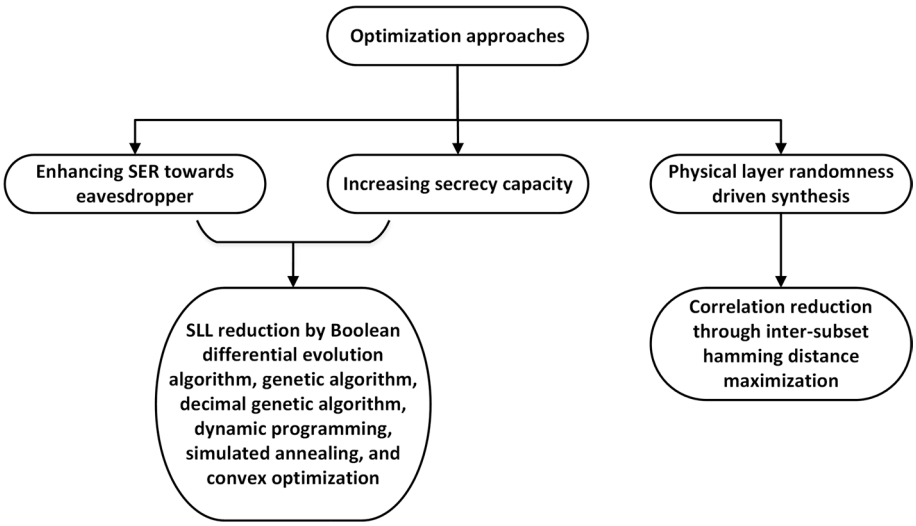

Fig. 6 In this figure, three broad categories of optimization approaches for increasing the physical layer security of directional modulation techniques available in the literature are summarized. The optimization goal from communications' paradigm is to increase symbol error rate in the direction of eavesdropper. Information-theoretic optimization maximizes the channel secrecy in the undesired directions. Finally, cryptographic viewpoint proposes physical layer randomness driven synthesis of directional modulation

One of the major limitations of angular DM techniques is that the legitimate user and adversary must be positioned along different angular directions. To make things worse, the direction of adversary always remains unknown since it is assumed to be passively eavesdropping. Authors in [68] have devised a new approach to overcome this issue by using multiple antenna arrays positioned at different spatial locations. It is called positional modulation. However, it comes at the cost of increased number of arrays which can be highly undesirable in certain applications. Alternatively, metasurface based positional modulation tries to cater for this issue by creating multipath communication channels through low-cost flexible reflecting surfaces [69]. Another interesting development is the use of intelligent reflecting surface (IRS) to create multipath for enhanced secrecy rate [70]. A detailed comparison along with performance metrics of angular DM techniques is provided in Table 3.

Different optimization approaches for spatial angular DM techniques are shown in Fig. 6. The most commonly used optimization approach in literature aims at increasing SER in unwanted directions of eavesdropper by SLL reduction. Different algorithms used for this purpose are; Boolean differential evolution algorithm [71], genetic algorithm (GA) [72], decimal GA [73], dynamic programming for unequally spaced arrays [74, 75], simulated annealing [76] and iterative convex optimization for multi-beam formation [77]. All these optimization algorithms are formulated purely from communications and information-theoretic paradigms, i.e. they are SNR-driven techniques. The goal of these techniques is to minimize the transmitted signal power in the direction of eavesdropper. Cryptographic randomness-driven synthesis of antenna arrays is presented in [57]. It proposes to increase the encryption strength by minimizing the correlation between successively used antennas subsets.

3.1.2 Temporal angular DM

The basic idea behind temporal angular DM is to divide the symbol duration into sub-slots of timing sequences and antenna array is modulated with respect to sub-slots of time. These techniques, also known as time-modulated array (TMA), are summarized in Tables 3 and 4. Based on TMA, a 4D antenna array has been proposed which uses time as the fourth dimension [78]. It has been demonstrated to achieve secure DM beam using BER and power patterns. One of the major challenges associated with 4D arrays is undesirably high SLL radiated power. This challenge has been addressed by designing optimized time sequences for SLL reduction [79]. The performance of 4D array is further enhanced by generating time-modulation based vector which provides improvement by distorting the vector information in the undesired directions [80]. The proposed design has been validated by hardware implementation and BER measurements.

Binary GA based synthesis of optimized on–off pulse sequence for TMA is proposed in [81]. It aims at maximizing distortion along the undesired directions. Subsequently, it was experimentally verified and its performance was quantified using fidelity rate to measure the amount of signal distortion and BER [82]. In [83], authors have combined TMA with traditional orthogonal frequency division multiplexing (OFDM) architecture to add another layer of security at physical interface. It performs better than OFDM in terms of BER, making it more secure against eavesdropping. Recently, multi-carrier DM based on careful design of time switching sequence of TMA has been proposed [84]. It achieves multi-carrier PLS at antenna level, unlike OFDM based TMA [83] in which is multi-carrier part is implemented at digital baseband.

3.1.3 Frequency angular DM

Frequency angular DM techniques use frequency parameter for achieving directional security. In [85], random subcarrier selection (RSCS) based DM for OFDM architecture has been proposed. The proposed scheme randomly modulates the subcarrier frequency for every symbol transmission after beam alignment along the required direction. The performance has been indicated in terms of SINR and secrecy rate. Discrete-Fourier transform (DFT) based angular DM is demonstrated to provide multi-directional secure communication for OFDM [86]. The DFT algorithm efficiently divides the antenna array to form multiple orthogonal sub-beams. Performance is measured in terms of power levels and average secrecy rate.

3.1.4 Phase angular DM

The phase dimension of antenna array can also be exploited to create DM at PHY layer [87]. In this technique, the phases are randomly adjusted when creating a directional beam towards the intended receiver. This architecture has been practically verified by authors in [88]. The idea is further extended to DM beamsteering of pattern-reconfigurable arrays [89]. A similar approach modulates the in-phase and quadrature-phase signals separately and use two separate antennas for each component. It effectively uses dual-beam for transmission of every symbol [90]. Furthermore, a hybrid technique of MIMO phased array is presented in [91] and polygon construction of DM phased array in [92].

3.1.5 Polarization angular DM

The use of polarization dimension for DM was first explored in [93]. In this approach, confidential information is concealed in carrier's polarization state. Crossed-dipole based antenna array implementation is presented in [94], in which orthogonally polarized carrier signals are transmitted at the same frequency but with different polarization states, effectively doubling the channel capacity. In [95], a directional polarization modulation architecture is presented for secure dual polarized satellite communication. Another recent development is polarization sensitive array (PSA) based angular DM [96]. The eavesdropper needs to estimate the exact polarization of the transmitter along with other DM parameters in order to recover originally transmitted signal.

3.2 Range-angular (2D) DM techniques

One of the interesting developments in DM is the exploitation of physical layer in such a way as to create two-fold security. The transmitted data is encrypted along two spatial dimensions, i.e. along range and angle. Accordingly, non-encrypted data is received only along pre-specified angular direction of receiver which has to be located at apriori-known distance range from the transmitter. The added layer of security in range dimension renders it more secure against eavesdropper compared to angular DM. For an eavesdropper to receive the original data, it has to be located not only along a certain direction but also at certain range from the transmitter, which is practically highly unlikely and difficult for eavesdropper. In the literature, frequency diverse array (FDA) and several of its variants have been proposed for secure range-angular DM [97]-[116]. FDA works at the core of all these methods. In our paper, we have classified these techniques based on the fundamental parameters which are being used to achieve PLS, namely; space, time, frequency and polarization. The detailed classification of 2D DM is shown in Fig. 3. An analysis from three security viewpoints is summarized in Table 5 and application specific comparison of these techniques in provided in Table 6.

3.2.1 Frequency range-angular DM

Originally inspired from radar signal processing, FDA exploits frequency dimension of PHY layer. In this approach, frequency increments are applied across the elements of the phased array. The resulting beampattern is a function of spatial range, spatial direction and time. One of the major issues in FDA is coupling of angle and range in far-field. This issue has been resolved by using nonlinear frequency increments [97]. However, performance evaluation has been conducted purely from communications paradigm using SINR, probability of detection and BER metrics. In FDA, it is highly desirable to achieve narrow-beam in the desired direction for minimum probability of eavesdropping. For this purpose, a narrower dot-shaped beampattern synthesis approach is presented in [98]. Range and angular power beampatterns are used to demonstrate the effectiveness of this approach.

Later on, the directional capability of FDA was extended by combining weighted fractional Fourier transform (WFRFT) with FDA [99]. It has the unique advantage over previous techniques as it can provide simultaneous multi-user secure communication. A similar approach uses singular value decomposition (SVD) to achieve the same

Table 5 Secure communication using range-angular DM techniques

Paper	Description	Communications parameters	Information-theoretic measures	Cryptographic strength
Frequency range-angular DM				
[97]	DM using frequency diverse array	SINR, probability of detection, BER	–	–
[98]	Dot-shaped beampattern synthesis of FDA	Beampatterns	–	–
[99]	WFRFT-aided multi-directional FDA	BER, robustness	Secrecy rate	–
[100]	SVD-aided multi-directional FDA	BER	Secrecy rate	–
[101]	FDA over Rayleigh fading channel	–	Secrecy capacity, secrecy outage probability	–
[102]	Frequency diverse subarray for fixed region beamforming	–	Secrecy rate	–
[103]	AN-aided FDA over Nakagami-m fading channel	–	Secrecy capacity	–
[104]	Multi-beam FDA based DM	BER	–	–
[105]	Multi-carrier FDA	BER	–	–
[106]	FDA for OFDM transmitter	BER	–	–
[107]	Genetic algorithm assisted beamforming for FDA	Peak-to-sidelobe ratio, MSE	–	–
[108]	AN-aided random FDA	–	Secrecy capacity	–
[109]	FDA using Butler matrix	BER	Secrecy capacity	–
[110]	Frequency index modulation for FDA	Beampatterns	–	–
[111]	Discular FDA	Beampatterns	–	–
Temporal range-angular DM				
[112]	Time-modulated FDA	BER	–	–
[113]	Time-invariant time-modulated FDA	BER	–	–
Spatial range-angular DM				
[114]	Antenna index modulation for FDA	Beampatterns	–	–
[115]	Quadrature spatial modulation based FDA	BER	Capacity analysis	–
Polarization range-angular DM				
[116]	Polarization sensitive beamforming for FDA	SINR, beampatterns	–	–

advantage over conventional FDA [100]. In both these papers, authors have used BER as well as secrecy capacity for performance analysis. However, cryptographic encryption strength analysis is missing. The derivation of exact expression of secrecy capacity for FDA and its analysis over Rayleigh fading channel is presented in [101]. This work has been extended to FDA subarrays for fixed region beamforming [102]. However, it is shown that Nakagami-m channel model for FDA is more realistic for such scenarios [103]. Recently proposed synthesis approaches use; multi-beam DM synthesis [104] and logarithmic increments of frequency [105] across the elements of phased array to achieve higher BER along eavesdropper. FDA has also been combined with existing OFDM transmitter [106] to provide another layer of security to existing architecture.

Table 6 Application specific comparison of range-angular DM techniques

S.no	Description	Applications
Frequency range-angular DM		
1	FDA based DM and its variants [97, 98, 101–103, 107–109]	Suitable for point-to-point applications in which both angular direction and range of the legitimate user are known to transmitter
2	Multi-directional FDA [99, 100, 104]	Enhanced directional capability of FDA is demonstrated. Particularly useful for multi-user FDA security applications
3	Multi-carrier FDA [105] [106]	Well-suited for integration with OFDM transmitters
4	Frequency index modulation for FDA [110]	Decoupling of range and angle is achieved for better security compared to simple FDA
5	Discular FDA [111]	Two-dimensional array geometry for FDA has been proposed. Suitable for applications in which secure transmission is required in a very narrow region of interest
Temporal range-angular DM		
6	Time-modulated FDA [112]	Resolves the issue of range-angular coupling in traditional FDA by time-modulation of antenna array
7	Time-invariant time-modulated FDA [113]	Logarithmic frequency offsets has been proposed to mitigate the time-variance issue associated with conventional FDA
Spatial range-angular DM		
8	Antenna index modulation for FDA [114]	Antenna array is both spatially modulated and diversified in frequency. This scheme not only enhances security but also increases throughput at the expense of increased receiver complexity
9	Quadrature spatial modulation based FDA [115]	A combination of QSM and FDA for enhanced security has been proposed
Polarization range-angular DM		
10	Polarization sensitive beamforming for FDA [116]	Polarization sensitive FDA technique provides not only range-angular security but also polarization dependent beam. An added complexity is the polarization control of array

There are several optimization approaches for FDA including; the use of genetic algorithm [107], random FDA for increased artificial noise [108] and Butler matrix for FDA [109]. The effect of genetic algorithm on FDA has been reflected on increased peak-to-sidelobe ratio (PSR) and MSE communications metrics in the undesired directions. The effect of using random FDA is measured in terms of secrecy capacity. However, Butler matrix optimization is analyzed in terms of both BER and secrecy capacity.

Another development proposes frequency sub-carrier index modulation for FDA [110]. The efficacy of proposed technique has been shown by comparing its beampatterns with conventional FDA and random offset based FDA. The advantage of modulating frequency sub-carrier index is decoupled range and angular dimensions. Moreover, it achieves higher data rates by additional information transmission on frequency offset

indices. A geometrical variation of FDA, namely discular FDA, proposes the use of planar disc instead of linear array geometry [111]. In this scheme, frequency offset is applied radially outwards. It has been shown that such geometry variation results in 3D dot-shaped beam pattern that can focus energy in a narrow spatial region of interest.

3.2.2 Temporal range-angular DM

As the name suggests, temporal range-angular DM combines the PHY layer dimension of time with FDA. In this technique, conventional FDA architecture is integrated with time-modulated array to create more diverse time-modulated FDA [112]. While this approach has the unique advantage of enhanced security in range dimension in comparison to simple time-modulated arrays, it also exhibits severe drawback of time-variance causing the range-angular beampattern to shift over time. This drawback is mitigated by using logarithmic frequency offsets and multi-carrier frequency offsets [113]. The resulting beampattern is secure and more robust in terms of time-invariance. The performance analysis of these techniques is limited to BER only as summarized in Table 5.

3.2.3 Spatial range-angular DM

Antenna index is a spatial dimension which can be exploited and combined with FDA to create robust DM transmission, as suggested in [114]. In this technique, a time-varying subset of antenna indices is selected and predefined frequency offsets are applied. One of the major issues associated with conventional FDA and its frequency variants is range-angle coupling. In this paper, it is shown that the resulting beampatterns have decoupled range-angle dimensions (an advantage over conventional FDA). This technique is suggested to be useful for FDA remote sensing applications as well. In [115], a hybrid of quadrature spatial modulation (QSM) and FDA has been proposed. In this technique, transmit information vector is mapped to antenna element indices. Moreover, in-phase and quadrature-phase components are transmitted at slightly different frequencies due to frequency offset nature of FDA. The resulting beam has secure range-angular DM properties as indicated by BER and capacity analysis.

3.2.4 Polarization range-angular DM

The range-angular DM techniques discussed so far utilize one particular antenna polarization state. However, the concept of FDA can also be combined with polarization dimension for more secure PHY layer data transmission. In fact, authors in [116] have presented similar idea of PSA based FDA to create polarization sensitive frequency diverse array (PSFDA). It has been shown through simulations that PSFDA provides lower SINR in the unwanted directions compared to conventional FDA.

4 Limitations, challenges and research directions

Although DM is a promising technology for secure future wireless communication networks, there are several limitations and challenges which need to be addressed as discussed below:

4.1 Angular DM techniques

The basic assumption in angular DM techniques is that eavesdropper is spatially located outside the main beam of antenna [50]. However, if eavesdropper is somehow located inside the main lobe of transmitter, angular DM techniques tend to fail. These techniques are successful only when augmented with security techniques of higher layers of communication protocol stack. Therefore, angular DM cannot completely replace baseband cryptographic encryption. However, architectural improvements on existing angular techniques and combining them with low cost cryptosystems can sufficiently reduce computational overheads associated with baseband encryption.

Another supposition is that the spatial direction of legitimate user with respect to transmitter is perfectly known. However, this may not be true in practical scenarios. The impact of imperfect angular estimation on the performance of spatial and DM techniques is studied in [118]. It is shown that imperfect angle estimation (IAE) implicates higher SNR requirement to achieve stable secrecy rate along the direction of eavesdropper. This issue merits further study. Moreover, this effect needs to be incorporated in future research.

SLL optimized antenna arrays have rather adverse effects on encryption strength, as shown in [56]. Although it has long been assumed in the literature that high SER is equivalent to high data security from communications perspective, this viewpoint is incompatible with cryptographic paradigm which is based on rigorous randomness driven analyses. Resolution of this conflict would be a critical and important step for unification of these security paradigms.

Practical implementation and evaluation of angular DM techniques is another research direction. There are no limitations in terms of electronics as high speed RF switches and other components at millimeter wave are readily available. Despite that, practical characterization and field testing of these techniques has not been conducted for most of the recently proposed schemes. Future developments in this direction is important because DM is one of the promising candidates for low-cost PLS deployment in 5G networks.

From the paradigm of cryptography, randomness-driven synthesis of angular DM techniques is a promising approach for attaining higher communication security.

As summarized in Table 4, there has been very little research in this direction. An examination of existing angular DM techniques from cryptographic perspective is required for an integrated PLS treatment.

Finally, physical limitations of angular DM techniques are another topic which merits further study. Associated with each antenna array, there are certain physical limitations beyond which the ideal assumptions fail to exist. There has been no research for accessing the physical limitations of angular DM.

4.2 Range-angular DM techniques

The study of range-angular DM is restricted only to communications and information-theoretic paradigms as evident in Table 5. Commonly used performance metrics in the literature are BER, SER, SINR and secrecy capacity. There has been no study from the paradigm of cryptography. With the advent of cryptographic analysis using certain physical layer mappings [56], adequate cryptographic tools are readily available to PLS researchers for analysis of range-angular DM techniques from this paradigm.

Recently, certain suspicions have raised about the security benefits of FDA [117]. It has been argued that there is a fundamental physical limitation of range dimension in FDA due to the propagation of secure reception region with time. It has been claimed that earlier research on FDA has overlooked this effect altogether. Careful examination of this issue would be an interesting development.

It can be observed in Fig. 3 that, unlike phased array based angular DM, there has been no study so far on the possibility of phase-variation in FDA. The incorporation of phase dimension with range-angular DM and its possible implications in terms of security benefits is an unexplored research avenue. PLS researchers have promising opportunity in this direction as well.

Finally, there has been very limited hardware validation of range-angular DM techniques. The future deployment of these techniques heavily relies upon their physical characterization, which is mostly limited to theoretical study. Resolution of these issues is necessary for practical utilization of DM techniques in wireless communication security.

5 Conclusion

In this paper, we have presented recent developments in directional modulation (DM) techniques for physical layer security (PLS). A new classification framework is proposed which is based on the extent of directional encryption, i.e. angular (1D) and range-angular (2D). For each category, further classification is performed using the specific physical layer parameters that are playing their role. DM techniques are studies from communications, information-theoretic and cryptographic paradigms. The subtle differences between these paradigms are highlighted. It is shown that researchers from these three fields are independently working on PLS and each one has their own developed set of tools and approaches which are shown to differ and sometimes contradict each other. This underscores the importance of unified treatment of PLS approaches. In the end, existing limitations of DM techniques are pointed out and future research directions are proposed.

Abbreviations

1D	One dimensional
2D	Two dimensional
AE	Approximate entropy test
AES	Advanced encryption standard
ASM	Antenna subset modulation
BER	Bit error rate
BK	Binary matrix rank test
BT	Block frequency test
CS	Cumulative sums test
DES	Data encryption standard
DFT	Discrete-Fourier transform
DM	Directional modulation
DOA	Direction of arrival
DT	Discrete Fourier transform test
EVM	Error vector magnitude
FFT	Fast-Fourier transform
FDA	Frequency diverse array
FT	Frequency monobits test
GA	Genetic algorithm
IAE	Imperfect angle estimation
IR	Intended receiver
ITP	Information-theoretic paradigm

IoT	Internet-of-things
LC	Linear complexity test
LR	Longest runs of ones in a block test
LSA	Linear sparse array
M2M	Machine-to-machine
MIMO	Multiple-input multiple-output
MIMOME	Multiple-input multiple-output multiple-eavesdropper
MISOME	Multiple-input single-output multiple-eavesdropper
MSE	Mean squared error
mmW	Millimeter wave
NFDAM	Near-field direct antenna modulation
NIST	National institute of standards and technology
NO	Non-Overlapping template matching test
NOMA	Non-orthogonal multiple access
OASS	Optimized antenna subset selection
OFDM	Orthogonal frequency division multiplexing
OV	Overlapping template matching test
PHY	Physical layer
PLS	Physical layer security
PLR	Physical layer randomness
PSA	Polarization sensitive array
PSK	Polarization shift keying
PSFDA	Polarization sensitive frequency diverse array
PSR	Peak-to-sidelobe ratio
QSM	Quadrature spatial modulation
RASS	Randomized antenna subset selection
RE	Random excursion test
RF	Radio frequency
RN	Runs test
RSA	Rivet Shamir Adelman
RSCS	Random sub-carrier selection
RMSE	Root mean-squared error
RV	Random excursion variant test
SAH	Silent antenna hopping
SER	Symbol error rate
SINR	Signal-to-interference-plus-noise ratio
SLL	Side-lobe level
SNR	Signal-to-noise ratio
SPA	Switched-phased-array
ST	Serial test
STS	Statistical test suite
SVD	Singular value decomposition
TMA	Time-modulated array
US	Universal statistical test
V2V	Vehicle-to-vehicle
WFRFT	Weighted fractional Fourier transform

Acknowledgements
Not applicable.

Author contributions
Following are the authors' original contributions: An updated survey of recent developments in DM techniques for physical layer data security in 5G wireless communication networks. Discussion and comparison of PLS from three different and seemingly independent paradigms; communications, information-theoretic approach, and cryptographic strength viewpoint, is presented. All the DM techniques in the literature have been classified based of parameters used for accessing their security performance from these different paradigms. This comparison shows that more integrated approach towards PLS and cryptography is required. Systematic classification of DM techniques based on their dimensional capability, i.e. angular DM (one-dimensional DM) and range-angular DM (two-dimensional DM). Furthermore, depending on the underlying technique used to achieve PLS, i.e. space, time, frequency, phase and polarization, a framework of classification based on generic parameters is proposed under each category. All the available techniques have been categorized under this framework. Moreover, all the future developments are very likely to lie under one (or a combination) of these classifications. All authors read and approved the final manuscript.

Author's information
Omar Ansari received the B.E. degree in electrical engineering from the University of Engineering and Technology, Taxila, Pakistan, in 2015, and graduated Summa Cum Laude in M.S. electrical engineering with specialization in RF and microwave from the Institute of Space Technology, Islamabad, Pakistan, in 2019.He is currently working as a Graduate Research Assistant with the Institute of Space Technology, where he is involved in the design and development of millimeter-wave front end for high altitude platform (HAP). His research interests include, but are not limited to, directional modulation techniques for physical layer security, antenna design, RF circuits, and electromagnetics.
Muhammad Amin received the B.E. degree in avionics from the PAF College of Aeronautical Engineering, NED University, Karachi, Pakistan, in 1988, the master's degree in electrical engineering with specialization inhigh-frequency techniques

from Ruhr University, Bochum, Germany, in 1998, and the Ph.D. degree from Queen's University Belfast (QUB), Belfast, U.K., in 2006. He taught as an Assistant Professor with the College of Electrical and Mechanical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan, from 1998 to 2002. He was a consultant with TDK Electronics to develop phased array antenna for automotive collision avoidance radar. He was a Research Fellow with QUB for approximately one year and an Associate Professor with the Institute of Space Technology (IST), Islamabad, Pakistan, from October 2007 to October 2009. From October 2009 to December 2014, he was the Head of the Antenna and EMI/EMC labs, Satellite Research and Development Centre, Lahore (SRDC-L), Pakistan, where he was involved in developing monopulse tracking system for satellite and EMI/EMC space qualification tests of the satellite communications system. Since 2015, he has been a Professor with IST, the Head of the Avionics Department, and the Director of the Cyber and Information Security Lab (CISL). His research interests include the development of antennas for radar and cellular communication systems, novel techniques for modulation, and RCS reduction. His research work has resulted in over 70 publications in major journals and refereed national and international conferences. He is the inventor of a lowest profile dual polarized antenna. He is mentioned in "Marquis Who is Who in the World" 2008 edition published in USA.

Funding
No funding was received to assist with the preparation of this manuscript.

Availability of data and materials
Not applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 18 December 2021 Accepted: 7 September 2022
Published online: 24 September 2022

References

1. H. Rifa-Pous, J. Herrera-Joancomartí, Computational and energy costs of cryptographic algorithms on handheld devices. Future Internet **3**, 31–48 (2011)
2. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, 2001)
3. M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge Univ Press, Cambridge, 2011)
4. D. Kapetanovic, G. Zheng, F. Rusek, Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. IEEE Commun. Mag. **53**(6), 21–27 (2015)
5. D. Steinmetzer, J. Chen, J. Classen, E. Knightly and M. Hollick, Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves, in IEEE conference on communications and network security (CNS), Florence, 2015, pp. 335–343
6. P. Sarankumar Balakrishnan, A.B. Wang, Z. Sun, On success probability of eavesdropping attackin 802.11ad mmWave WLAN", in IEEE international conference on communications (ICC), 2018, pp. 1–6
7. P. Sarankumar Balakrishnan, A.B. Wang, Z. Sun, Modeling and analysis of eavesdropping attack in 802.11ad mmWave wireless networks. Access IEEE **7**, 70355–70370 (2019)
8. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M.D. Renzo, Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. **53**(4), 20–27 (2015)
9. X. Chen, D.W.K. Ng, W.H. Gerstacker, H.-H. Chen, A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutor. **19**(2), 1027–1053 (2017)
10. Y. Liu, H. Chen, L. Wang, Physical layer security for next generation wireless networks: theories, technologies, and challenges. IEEE Commun. Surv. Tutor. **19**(1), 347–376 (2017)
11. Wu. Yongpeng, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J. Select. Areas Commun. **36**(4), 679–695 (2018)
12. I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5G and beyond. IEEE Commun. Surv. Tutor. **21**(4), 3682–3722 (2019)
13. J.M. Hamamreh, H.M. Furqan, H. Arslan, Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1773–1828 (2019)
14. D. Wang, B. Bai, W. Zhao, Z. Han, A survey of optimization approaches for wireless physical layer security. IEEE Commun. Surv. Tutor. **21**(2), 1878–1911 (2019)
15. B. Li, Z. Fei, C. Zhou, Y. Zhang, Physical-layer security in space information networks: a survey. IEEE Internet Things J. **7**(1), 33–52 (2020)
16. Y. Ding, V.F. Fusco, A review of directional modulation technology. Int. J. Microw. Wirel. Technol. **8**(7), 981–993 (2016)
17. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
18. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1367 (1975)

19. S.K. Leung-Yan-Cheong, M.E. Hellman, The gaussian wire-tap channel. IEEE Trans. Inf. Theory **24**(4), 451–456 (1978)
20. I. Csiszar, J. Korner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1978)
21. D. He, W. Guo, Y. Luo, Secrecy capacity of the extended wiretap channel II with noise. Entropy **18**, 377 (2016)
22. A. Ahmad, M. Amin and M. Farooq M, Analyzing directional modulation techniques as block encryption ciphersfor physical layer security," in IEEE wireless communications and networking conference (WCNC), San Francisco, CA, 2017
23. Y. Huang, W. Li, J. Lei, Concatenated physical layer encryption scheme based on rateless codes. IET Commun. **12**(12), 1491–1497 (2018)
24. E.R. Tollefson, B.R. Jordan, Physical layer encryption using out-phased array linearized signaling, US Patent 10225039, 2015
25. E. Tollefson, B.R. Jordan and J.D. Gaeddert, Out-phased array linearized signaling (OPALS): A practical approach to physical layer encryption, in MILCOM—IEEE military communications conference, Tampa, FL, 2015, pp. 294–299
26. Y. Huang, J. Lei, M. El-Hajjar, W. Li, Multi-dimensional encryption scheme based on physical layer for fading channel. IET Commun. **12**(19), 2470–2477 (2018)
27. S. Huang, Y. Gao, H. Xi, N. Sha, A physical layer encryption scheme based on symbol convolution for MISO secure transmission, in IEEE 19th international conference on communication technology (ICCT), 2019, pp. 290–295
28. E. Baghdady, Directional signal modulation by means of switched spaced antennas. IEEE Trans. Commun. **38**, 399–403 (1990)
29. Y. Ding, V. Fusco, Development in directional modulation technology. Forum Electromagn. Res. Methods Appl. Technol. **13**, 1–7 (2016)
30. Y. Ding, V. Fusco, Establishing metrics for assessing the performance of directional modulation systems. IEEE Trans. Antennas Propag. **62**(5), 2745–2755 (2014)
31. Y. Ding, V. Fusco, A vector approach for the analysis and synthesis of directional modulation transmitters. IEEE Trans. Antennas Propag. **62**(1), 361–370 (2014)
32. A.O. Hero, Secure space-time communication. IEEE Trans. Inf. Theory **49**(12), 3235–3249 (2003)
33. T. Liu, S. Shamai, A note on the secrecy capacity of the multiantenna wiretap channel. IEEE Trans. Inf. Theory **55**(6), 2547–2553 (2009)
34. A. Khisti, G.W. Wornell, Secure transmission with multiple antennas-I: the MISOME wiretap channel. IEEE Trans. Inf. Theory **56**(7), 3088–3104 (2010)
35. A. Khisti, G.W. Wornell, Secure transmission with multiple antennas—part II: the MIMOME wiretap channel. IEEE Trans. Inf. Theory **56**(11), 5515–5532 (2010)
36. F. Oggier, B. Hassibi, The secrecy capacity of the MIMO wiretap channel. IEEE Trans. Inf. Theory **57**(8), 4961–4972 (2011)
37. A. Salomaa, *Public Key Cryptography* (Springer, New York, 1996)
38. R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM **21**, 120–126 (1978)
39. H. Seung-Jo, O. Heang-Soo, and P. Jongan, The improved data encryption standard (DES) algorithm, in 4th international symposium on spread spectrum techniques and applications, IEEE, 3, 1310-1314, 1996
40. Announcing the Advanced Encryption Standard (AES), Federal information processing standards publication 197, November 26, 2001
41. M. Bellare, S. Tessaro, A. Vardy, A cryptographic treatment of the wiretap channel", arXiv:1201.2205, 2012
42. M. Sys, Z. Riha, Faster randomness testing with the NIST statistical test suite, in security, privacy, andapplied cryptography engineering, LNCS 8804, 2014, pp. 272–284
43. Brown R. G., Dieharder: A Random Number Test Suite, Version 3.31.1, 2004
44. P. Lecuyer, R. Simard, TestU01: A C library for empirical testing of random number generators. ACM Trans. Math. Softw. **33**(4), 1–40 (2007)
45. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST special publication, 2010
46. D. Muedoch, Y. Tsai, J. Adcock, P-values are random variables. Am. Stat. **62**, 242–245 (2008)
47. E.L. Lehmann, *Testing Statistical Hypotheses* (John Wiley Sons, New York, 1969)
48. J.J. Soto, Randomness testing of the advanced encryption standard candidate algorithms, National Institute of Standards and Technology, 1999
49. N. Valliappan, R.W. Heath Jr., and A. Lozano, Antenna subset modulation for secure millimeter-wave wireless communication, in Globecom workshops (GC Wkshps), 2013, pp. 1258–1263
50. N. Valliappan, A. Lozano, R.W. Heath Jr., Antenna subset modulation for secure millimeter-wave wireless communication. IEEE Trans. Commun. **61**(8), 3231–3245 (2013)
51. N.N. Alotaibi and K.A. Hamdi, A low-complexity antenna subset modulation for secure millimeterwave communication, in 2016 IEEE wireless communications and networking conference, 2016, pp 1–6
52. C. Rusu, N. Gonzalez-Prelcic, and R. Heath, An attack on antenna subset modulation for millimeter wave communication, in IEEE international conference on acoustics, speech and signal processing (ICASSP), April 2015, pp. 2914–2918
53. C. Chen et al., An iterative FFT-based antenna subset modulation for secure millimeter wave communications, in Proc IEEE ICNC, Silicon Valley, CA, USA, 2017, pp. 454–459
54. M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri and R. W. Heath, On the security of millimeter wave vehicular communication systems using random antenna subsets, in IEEE 84th vehicular technology conference (VTC-Fall), Montreal, QC, 2016, pp. 1–5
55. M. Eltayeb, J. Choi, T.Y. Al-Naffouri, R.W. Heath Jr., Enhancing secrecy with multi-antenna transmission in millimeter wave vehicular communication systems. IEEE Trans. Veh. Tech. **66**(9), 8139–8151 (2017)
56. O. Ansari, M. Amin, A. Ahmad, Analyzing physical layer security of antenna subset modulation as block encryption ciphers. IEEE Access **7**, 185063–185075 (2019)

57. O. Ansari, M. Amin, M. Maqsood, A.R.M. Maud, M. Farooq, Inter-subset hamming distance maximization for enhancing the physical layer security of antenna subset modulation. IEEE Access **8**, 221513–221524 (2020)
58. T. Hong et al., RF directional modulation technique using a switched antenna array for physical layer secure communication applications. Prog. Electromag. Res. **116**, 363–379 (2011)
59. N.N. Alotaibi, K.A. Hamdi, Switched phased-array transmission architecture for secure millimeter-wave wireless communication. IEEE Trans. Commun. **64**(3), 1303–1312 (2016)
60. N.N. Alotaibi, K.A. Hamdi, Silent antenna hopping transmission technique for secure millimeter-wave wireless communication, in Proc. IEEE GLOBECOM, 2015, pp. 1–6
61. F. Liu, L. Wang, J. Xie, Directional modulation technique for linear sparse arrays. IEEE Access **7**, 13230–13240 (2019)
62. T. Hong, X.-P. Shi, X.-S. Liang, Synthesis of sparse linear array for directional modulation via convex optimization. IEEE Trans. Antennas Propag. **66**(8), 3959–3972 (2018)
63. Y. Ding, V. Fusco, A. Chepala, Circular directional modulation transmitter array. IET Microw. Antennas Propag. **11**(13), 1909–1917 (2017)
64. Y. Ding, V. Fusco, A synthesis-free directional modulation transmitter using retrodirective array. IEEE J. Sel. Top. Signal Process. **11**(2), 428–441 (2017)
65. X. Lu, S. Venkatesh, B. Tang, K. Sengupta, 4.6 space-time modulated 71-to-76 GHz mm-Wave transmitter array for physically secure directional wireless links, in IEEE international solid-state circuits conference - (ISSCC), 2020, pp. 86–88
66. A. Babakhani, D.B. Rutledge, A. Hajimiri, Near-field direct antenna modulation. IEEE Microw. Mag. **10**(1), 36–46 (2009)
67. A. Babakhani, D. Rutledge, A. Hajimiri, Transmitter architectures based on near-field direct antenna modulation. IEEE J. Solid-State Circuits **43**, 2674–2692 (2008)
68. B. Zhang, W. Liu, Positional modulation design based on multiple phased antenna arrays. IEEE Access **7**, 33898–33905 (2019)
69. B. Zhang et al., Sparse antenna array based positional modulation design with a low-complexity metasurface. IEEE Access **8**, 177640–177646 (2020)
70. F. Shu et al., Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
71. L. Zhang, Y.-C. Jiao, Z.-B. Weng, F.-S. Zhang, Design of planar thinned arrays using a Boolean differential evolution algorithm. IET Microw. Antennas Propag. **4**(12), 2172–2178 (2010)
72. R. Haupt, Thinned arrays using genetic algorithms. IEEE Trans. Antennas Propag. **42**(7), 993–999 (1994)
73. M.T. Ali, R. Abdolee, T.A. Rahman, Decimal genetics algorithms for null steering and sidelobe cancellation in switch beam smart antenna system. Int. J. Comput. Sci. Secur. **1**(3), 19–26 (2007)
74. M. Skolnik, G. Nemhauser, J. Sherman, Dynamic programming applied to unequally spaced arrays. IEEE Trans. Antennas Propag. **12**, 35–43 (1964)
75. R. Arora, N. Krisnamacharyulu, Synthesis of unequally spaced arrays using dynamic programming. IEEE Trans. Antennas Propag. **16**, 593–595 (1968)
76. V. Murino, A. Trucco, C.S. Regazzoni, Synthesis of unequally spaced arrays by simulated annealing. IEEE Trans. Signal Process. **44**(1), 119–123 (1996)
77. R.M. Christopher, D.K. Borah, Iterative convex optimization of multi-beam directional modulation with artificial noise. IEEE Commun. Lett. **22**(8), 1712–1715 (2018)
78. Q. Zhu et al., Directional modulation based on 4-D antenna arrays. IEEE Trans. Antenna Prop. **62**(2), 621–628 (2014)
79. K. Chen, S. Yang, Y. Chen, S.-W. Qu, J. Hu, Hybrid directional modulation and beamforming for physical layer security improvement through 4-D antenna arrays. IEEE Trans. Antennas Propag. **69**(9), 5903–5912 (2021)
80. C. Qu et al., A vector modulation approach for secure communications Based on 4-d antenna arrays. IEEE Trans. Antennas Propag. **70**(5), 3723–3732 (2022)
81. M.A. Hannan, L. Poli, P. Rocca, and A. Massa, Pulse sequence optimization in time-modulated arrays for secure communications, in Proc. IEEE Int. Symp. Antennas Prop. (IEEE AP-S 2016) and USNC/URSI Nat. Radio Sci. Meeting, Fajardo, Puerto Rico, 2016, pp. 695–696
82. J. Guo, L. Poli, M.A. Hannan, P. Rocca, S. Yang, A. Massa, Time-modulated arrays for physical layer secure communications: optimization-based synthesis and experimental assessment. IEEE Trans. Antennas Propag. **66**(12), 6939–6949 (2018)
83. Y. Ding, V. Fusco, J. Zhang, W. Wang, Time-modulated OFDM directional modulation transmitters. IEEE Trans. Veh. Technol. **68**(8), 8249–8253 (2019)
84. G. Huang, Y. Ding, S. Ouyang, Multicarrier directional modulation symbol synthesis using time-modulated phased arrays. IEEE Antennas Wirel. Propag. Lett. **20**(4), 567–571 (2021)
85. F. Shu, X. Wu, J. Hu, J. Li, R. Chen, J. Wang, Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array. IEEE J. Sel. Areas Commun. **36**(4), 890–904 (2018)
86. M. Hafez, T. Khattab, H. Arslan, DFT-based multi-directions directional modulation. IEEE Wirel. Commun. Lett. **8**(4), 1232–1235 (2019)
87. M. Daly, J. Bernhard, Directional modulation technique for phased arrays. IEEE Trans. Antennas Propag. **57**, 2633–2640 (2009)
88. M. Daly, E. Daly, J. Bernhard, Demonstration of directional modulation using a phased array. IEEE Trans. Antennas Propag. **58**, 1545–1550 (2010)
89. M. Daly, J. Bernhard, Beamsteering in pattern reconfigurable arrays using directional modulation. IEEE Trans. Antennas Propag. **58**, 2259–2265 (2010)
90. T. Hong, M.-Z. Song, Y. Liu, Dual-beam directional modulation technique for physical-layer secure communication. IEEE Antennas Wirel. Propag. Lett. **10**, 1417–1420 (2011)
91. W.-Q. Wang, Z. Zheng, Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications. J. Select. Areas Commun. IEEE **36**(7), 1383–1396 (2018)

92. X. Zhang, X.-G. Xia, Z. He, X. Zhang, Phased-array transmission for secure mmWave wireless communication via polygon construction. IEEE Trans. Signal Process. **68**, 327–342 (2020)
93. Dong Wei, Lili Liang, Meng Zhang, Rong Qiao and Weiqing Huang, A polarization state modulation based physical layer security scheme for wireless communications, in MILCOM 2016 - 2016 IEEE military communications conference, 2016, pp. 1195–1201
94. B. Zhang, W. Liu, X. Lan, Orthogonally polarized dual-channel directional modulation based on crossed-dipole arrays. IEEE Access **7**, 34198–34206 (2019)
95. Q. Zhang, Z. Yang, W. Wang, J. Ren, W. Huang and N. Zhang, A dual-polarized antennas based directional modulation Scheme, in 26th international conference on telecommunications (ICT), 2019
96. W. Zhang, B. Li, M. Le, J. Wang, J. Peng, Directional modulation technique Using a polarization sensitive array for physical layer security enhancement. Sensors **19**(24), 5396 (2019). (**Basel**)
97. W.Q. Wang, DM using FDA antenna for secure transmission". IET Microw. Antennas Propag **11**(3), 336–345 (2017)
98. H. Shao, J. Dai, J. Xiong, H. Chen, W.-Q. Wang, Dot-shaped range-angle beampattern synthesis for frequency diverse array. IEEE Ante. Wirel. Propag. Lett. **15**, 1703–1706 (2016)
99. Q. Cheng, V. Fusco, J. Zhu, S. Wang, F. Wang, WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array. IEEE Trans. Wirel. Commun. **18**(11), 5211–5226 (2019)
100. Q. Cheng, V. Fusco, J. Zhu, S. Wang, Gu. Chao, SVD-aided multi-beam directional modulation scheme based on frequency diverse array. IEEE Wirel. Commun. Lett. **9**(3), 420–423 (2020)
101. S. Ji, W.-Q. Wang, H. Chen, S. Zhang, On physical-layer security of FDA communications over Rayleigh fading channels. IEEE Trans. Cogn. Commun. Netw. **5**(3), 476–490 (2019)
102. Y. Hong, X. Jing, H. Gao, Y. He, Fixed region beamforming using frequency diverse subarray for secure mmWave wireless communications. IEEE Trans. Inform. Forensic Secur. **15**, 2706–2721 (2020)
103. S. Ji, W. Wang, H. Chen, Z. Zheng, Secrecy capacity analysis of AN-aided FDA communication over Nakagami-m fading. IEEE Wirel. Commun. Lett. **7**(6), 1034–1037 (2018)
104. B. Qiu, M. Tao, L. Wang, J. Xie, Y. Wang, Multi-beam directional modulation synthesis scheme based on frequency diverse array. IEEE Trans. Info. Forensics Secur. **14**(10), 2593–2606 (2019)
105. T. Xie, J. Zhu, Q. Cheng, J. Luo, Secure directional modulation using the symmetrical multi-carrier frequency diverse array with logarithmical frequency increment. IEICE Trans. Fundam. Electro. Commun. Comput. Sci. **4**, 633–640 (2019)
106. Y. Ding, V. Fusco, J. Zhang, Frequency diverse array OFDM transmitter for secure wireless communication. Electron. Lett. **51**(17), 1374–1376 (2015)
107. J. Xiong, W.-Q. Wang, H. Shao, H. Chen, Frequency diverse array transmit beampattern optimization with genetic algorithm. IEEE Antennas Wirel. Propag. Lett. **16**, 469–472 (2017)
108. J. Hu, S. Yan, F. Shu, J. Wang, J. Li, Y. Zhang, Artificial-Noise-Aided secure transmission with directional modulation based on random frequency diverse arrays. IEEE Access **5**, 1658–1667 (2017)
109. S.Y. Nusenu, H. Chen, W. Wang, S. Ji, O. Opuni-Boachie, Frequency diverse array using butler matrix for secure wireless communications. Prog. Electromagn. Res. **63**, 207–215 (2018)
110. G. Huang, S. Ouyang, Y. Ding, V. Fusco, Index modulation for frequency diverse array. IEEE Antennas Wirel. Propag. Lett. **19**(1), 49–53 (2020)
111. A. Akkoc, E. Afacan, E. Yazgan, Dot-shaped 3D range-angle dependent beamforming with discular frequency diverse array. IEEE Trans. Antennas Propag. **69**(10), 6500–6508 (2021)
112. S.Y. Nusenu, W.Q. Wang, J. Xiong, Time-modulated frequency diverse array for physical-layer security. IET Microw Antennas Propag **11**(9), 1274–1279 (2017)
113. Q. Cheng, J. Zhu, T. Xie, J. Luo, Z. Xu, Time-invariant angle-range dependent directional modulation based on time modulated frequency diverse arrays. IEEE Access **5**, 26279–26290 (2017)
114. G. Huang, Y. Ding, V. Fusco, S. Ouyang, Antenna element index modulation for frequency diverse array. Int. J. Antennas Propag. **2019**, 1–8 (2019)
115. A. Basit, W.-Q. Wang, S.Y. Nusenu, S. Wali, FDA based QSM for mmWave wireless communications: frequency diverse transmitter and reduced complexity receiver. IEEE Trans. Wirel. Commun. **20**(7), 4571–4584 (2021)
116. H. Chen, H. Shao, H. Chen, Angle-range-polarization-dependent beamforming for polarization sensitive frequency diverse array. EURASIP J. Adv. Signal Process. **2019**(1), 1–4 (2019)
117. Y. Ding, A. Narbudowicz, G. Goussetis, Physical limitation of range-domain secrecy using frequency diverse arrays. IEEE Access **8**, 63302–63309 (2020)
118. H. Zhang, Y. Xiao, Y. Xiao, W. Xiang, Impact of imperfect angle estimation on spatial and directional modulation. IEEE Access **8**, 7081–7092 (2020)

Publisher's Note