This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

Low-Complexity Dynamic Directional Modulation: Vulnerability and Information Leakage

Pedro E. Gória Silva, Adam Narbudowicz, *Senior Member, IEEE*, Nicola Marchetti, *Senior Member, IEEE*, Pedro H. J. Nardelli, *Senior Member, IEEE*, Rausley A. A. de Souza, *Senior Member, IEEE*, and Jules M. Moualeu, *Senior Member, IEEE*

***Abstract*—In this paper, the privacy of wireless transmissions is improved through an efficient technique termed dynamic directional modulation (DDM) and is subsequently assessed in terms of the measure of information leakage. Recently, a variation of DDM termed low-power dynamic directional modulation (LPDDM) has attracted significant attention as a prominent secure transmission method owing to its ability to improve the privacy of wireless communications. Roughly speaking, this modulation operates by randomly selecting the transmitting antenna from an antenna array whose radiation pattern is known. Thereafter, the modulator adjusts the constellation phase so as to ensure that only the legitimate receiver recovers the information. To begin with, we highlight some privacy boundaries inherent to the underlying system. In addition, we propose features that the antenna array must meet in order to increase the privacy of a wireless communication system. Last, we adopt a uniform circular monopole antenna array with equiprobable transmitting antennas in order to assess the impact of DDM on information leakage and the bit error rate (BER).**

***Index Terms*—Physical layer security, information leakage, directional modulation, phased array, antenna array.**

I. Introduction

In recent years, physical layer security (PLS) has attracted much attention from the research community as a promising technology for securing communications over wireless channels (see [1]–[3] and the references therein). In contrast to the traditional approach, which addresses information security through mathematically derived encryption techniques in the upper layers of the wireless network protocol stacks, PLS or information-theoretic security is implemented at the lowest layer of the Open System Interconnect (OSI) stack, i.e., the physical layer. It exploits the unique physical features of wireless propagation channels to prevent the information being obtained by unintended receivers through eavesdropping or malicious attacks [4]–[7]. Owing to its promising benefits, PLS has been widely investigated in the literature as a potential candidate to safeguard fifth-generation (5G) and beyond wireless communications, complementing the encryption-based method. However, there are drawbacks associated with the PLS implementation, such as the significant memory consumption, which may impose strict requirements on wireless devices in the context of 5G technology [8].

A recent PLS technique referred to as directional modulation (DM) (see [9]–[12] and the references therein) has emerged as an efficient and secure transmission approach suitable for wireless communications, including millimeter-wave (mmWave), unmanned aerial vehicles (UAV), satellite communication, and smart transportation [13], [14]. DM has the potential to steer the intended baseband information in the desired direction while transmitting distorted signals in other directions. Specifically, the original information-bearing signal is only transmitted in a narrow directive beam toward the intended user. The genesis of DM stems from [9], which uses phased arrays (PA) to improve security as long as the eavesdropper is not in the same direction as the legitimate receiver.

Recent studies have revealed a high complexity for combining an antenna array with complex signal processing techniques. For instance, the authors in [15] propose a zero-forcing (ZF) technique to reduce the computational complexity of DM; although the proposed solution addresses the complexity issue, it comes at the expense of a large antenna array. The works [11], [16] propose means to miniaturize the antenna array but at the cost of hardware complexity since the system requires individual amplitude and phase control over each port and additional radio frequency (RF) chains. The authors in [17] synthesize multicarrier directional modulation symbols for PLS through a meticulous design of a time-switching sequence and time-modulated PA. However, this approach is impractical for Internet of Things (IoT) devices or other low-cost devices because of the high complexity deriving

P. E. G. Silva and P. H. J. Nardelli are with Lappeenranta–Lahti University of Technology, Finland (email: pedro.goria.silva@lut.fi, pedro.nardelli@lut.fi). P. E. G. Silva is also with INATEL, Brazil. P. H. J. Nardelli is also with University of Oulu, Finland.
A. Narbudowicz and N. Marchetti are with Trinity College Dublin, Ireland (email:narbudoa; nicola.marchetti@tcd.ie). A. Narbudowicz is also working part-time with Wroclaw University of Science and Technology, Wroclaw, Poland.
R. A. A. de Souza is with National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí 37540-000, Brazil (e-mail: rausley@inatel.br).
J. M. Moualeu is with the University of the Witwatersrand, Johannesburg, South Africa (e-mail: jules.moualeu@wits.ac.za). J. M. Moualeu was with the Lappeenranta–Lahti University of Technology on a research visit at the completion of this research.
This paper is partly supported by the Academy of Finland via: (a) FIREMAN consortium n.326270 as part of CHIST-ERA grant CHIST-ERA-17-BDSI-003, (b) EnergyNet Fellowship n.321265/n.328869/n.352654, (c) X-SDEN project n.349965, and (d) Science Foundation Ireland under grant 13/RC/2077_P2 (CONNECT); by CNPq (Grant References 311470/2021-1 and 403827/2021-3; by São Paulo Research Foundation (FAPESP) (Grant No. 2021/06946-0); by RNP, with resources from MCTIC, Grant No. 01245.020548/2021-07, under the Brazil 6G project of the Radiocommunication Reference Center (Centro de Referência em Radiocomunicações - CRR) of the National Institute of Telecommunications (Instituto Nacional de Telecomunicações - Inatel), Brazil; by Huawei, under the project Advanced Academic Education in Telecommunications Networks and Systems, contract No PPA6001BRA23032110257684; and by by the National Research Foundation (NRF) of South Africa under the BRICS Multilateral Research and Development Project (Grant No. 116018); and by Business Finland under the project REEVA (n.10278/31/2022).

from the synchronization with high-degree accuracy in the switching mechanism [18]. Similarly to [17], [7] proposes a practical and simplified scheme for IoT devices that provides energy efficiency and cost-effectiveness through a single RF chain and an array of closely spaced antennas. It requires a switchable antenna array and a random number generator at the transmitter, along with a simple receiver. Moreover, it does not introduce additional artificial noise in the direction of the legitimate receiver.

Despite the growing interest in DM-based PLS transmission, the existing literature has evaluated only a few metrics. In [10], the authors assess error vector magnitude (EVM), bit error rate (BER), and secrecy rate (SR). EVM calculates the normalized mean of the square of the difference between the measured streams and the reference symbols in the in-phase and quadrature (IQ) space. It is commonly adopted to quantify the system performance without executing the demodulation process and to distinguish physical sources from distortion. Albeit BER, EVM, and SR are equivalent for dynamic DM systems under the assumption of a zero-mean Gaussian distributed orthogonal interference, the authors in [10] point out a discrepancy between such metrics for static DM systems. Recently, several studies have used BER or a variation of SR as a metric to evaluate the system performance [7], [8], [11], [19]. In [8], the system performance is evaluated in terms of average secrecy capacity (ASC), secrecy outage probability (SOP), and BER. It is worthwhile recalling the dependence of both the ASC and the SOP on the SR, which is intrinsically linked to mutual information. However, mutual information is not an adequate security metric[1]. A closely related work to our proposed study is [7], where a uniform circular array of monopole antennas with equiprobable transmitting antennas is proposed. In that work, Narbudowicz *et al.* show that the privacy of wireless communication can be achieved by randomly switching the transmitting antenna. Furthermore, the authors rely on BER as a performance metric to evaluate the privacy of the system.

Motivated by the preceding discussion, our proposed work aims at adopting other performance metrics as a means to evaluate the security of a wireless communication system in terms of vulnerability. Our approach is prompted by the inefficacy of the BER (equivalent to EVM and SR for dynamic DM systems [10]) in conjunction with trivial demodulation—this procedure has been widely adopted in the technical literature as a security performance metric for wireless communications, e.g., in [8], [11], [19] in gauging information leakage. To the best of the authors' knowledge, our work is the first that adopts a theoretical approach to information and security for the DM scheme. The contributions of this work are as follows:

- We highlight some privacy boundaries inherent to the underlying system and provide insights into how an eavesdropper can intercept confidential information intended for a legitimate receiver.
- We propose a design of an antenna array that minimizes the system vulnerability for an acceptable level of privacy. More precisely, we show that the system vulnerability can be significantly reduced for a large number of transmitting antennas. Moreover, we derive the fundamental limits of the system vulnerability.
- We adopt a uniform circular monopole antenna array with equiprobable transmitting antennas and then evaluate its impact on the measure of information leakage. Furthermore, we demonstrate how the transmission of constellations can ensure privacy in the context of data confidentiality.

[1]This will be subsequently discussed in the manuscript.

The rest of the paper is organized as follows. The system model is described in Section II, and the proposed vulnerability approach is elaborated in Section III. Section IV presents the theoretical limits of the proposed system, and discusses the antenna array design that minimizes the information leakage. A case study is investigated and numerical results are illustrated in Section V. Finally, Section VI provides some concluding remarks.

II. System Model

The energy-efficient DM system proposed in [7] consists of a standard modulator, a phase delayer, a circular antenna array, and a random integer generator. The block diagram of the system and the phase displacement are presented in Fig. 1. The standard modulator block performs IQ modulation of the data. It is worth mentioning that phase-based modulation (e.g., M-ary phase-shift keying or quadrature amplitude modulation) represents the worst-case scenario for eavesdroppers to perform a successful attack; in brief, the security of the DM scheme is based on phase distortion, and thus, modulations whose information is not somehow contained in a phase are more susceptible to a successful attack. For the sake of simplicity, we assume that the phase displacement at the modulator output is null. Let $\theta_n(\phi)$ be the phase shift generated by the radiation pattern (including the displacement) of the nth antenna in the direction ϕ. The phase delay rotates the symbol by $\theta_{\mathrm{DM}}(\phi_{\mathrm{Bob}}, n)$ radians, with ϕ_{Bob} and $n \in \{1, 2, \ldots, N\}$ being the direction of the legitimate (intended) receiver and the transmitting antenna, respectively. For the proposed DM scheme, this phase shift added to the phase delay block is given by

$$\theta_{\mathrm{DM}}(\phi_{\mathrm{Bob}}, n) = -\theta_n(\phi_{\mathrm{Bob}}). \tag{1}$$

The phase delay block works as a predistortion phase of the transmitted signal, which allows its correct reconstruction only along the intended direction ϕ_{Bob}. Therefore, the total phase shift at the receiver is given by

$$\theta_{\mathrm{Rx}}(\phi, n) = \theta_{\mathrm{DM}}(\phi_{\mathrm{Bob}}, n) + \theta_n(\phi) + \theta_{\mathrm{Ch},n}, \tag{2}$$

where $\theta_{\mathrm{Ch},n}$ is defined as the phase shift of the channel between the nth antenna and the receiver, as indicated in Fig. 1. Hereafter, we will omit the $\theta_{\mathrm{Ch,n}}$ dependence on the transmitting antenna n in order to simplify the notation. Note that $\theta_{\mathrm{Ch},n} \forall n \in 1, 2, \ldots, N$ are statistically identical. After substituting (1) into (2), it can be seen that the phase shift from the phase delay block and the antenna array cancel each other out in the direction $\phi = \phi_{\mathrm{Bob}}$, leaving the phase shift at the legitimate receiver to be caused exclusively by

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

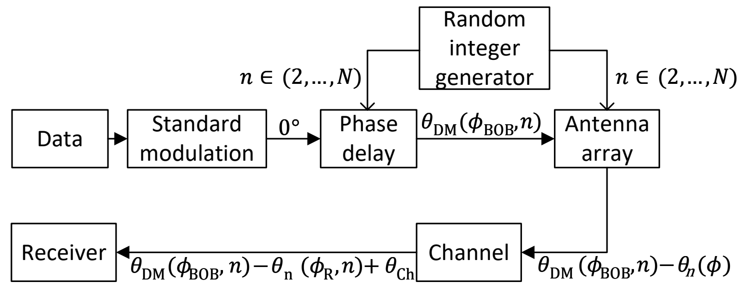

Fig. 1. Block diagram of the energy-efficient DM system.

the channel delay. On the other hand, there is an additional phase component that changes as a function of the direction ϕ, leading to the distortion of the transmitted signal for $\phi \neq \phi_{\text{Bob}}$—with the severity of the distortion being dependent on the antenna array design.

However, if the eavesdropper obtains information about the radiation pattern used, it can somehow compensate for the additional phase shift. The system aims to preclude this by randomly switching between different antennas in the array, i.e., it is the primary function of the random integer generator. In this way, the eavesdropper cannot squarely distinguish the phase artificially generated by the DM system from the phase modulation. Therefore, the system may provide a certain level of security for the secret information while transmitting via only one antenna at each given time; the other antennas of the array remain disconnected. Thus, we can use a single RF chain leading to a significant hardware simplification compared with other DM schemes [7]. Before the data transmission phase, most wireless systems require a handshake. Here, the transmitter and the legitimate receiver perform a handshake through a reference antenna n_{R}, which is not used later for data transmission. Hereafter, we will assume that the antenna array is composed of $N+1$ antennas in such a way that we have the transmitting antenna $n \in \{1, 2, \ldots, N\}$; in the sequel, when referring to the antenna array, we allude to the N antennas usable in the transmission phase after the handshake.

In a nutshell, the transmission method consists of the following chronological sequence of actions: 1) modulate the data using any modulation pattern; 2) randomly select a transmitting antenna for each new symbol; 3) correct the symbol phase based on the drawn antenna; 4) transmit the symbol with the corrected phase.

In order to facilitate the visualization of the transmission procedure, we present Algorithm 1 that exemplifies how to generate L output symbols given $L \times 2$ input bits with a QPSK modulation. Note that the legitimate receiver can trivially demodulate the received signal.

Algorithm 1 Complex symbol transmitted in the direction ϕ with the energy-efficient DM

Require: $Data \in \{0,1\}^{L\times 2}$
Ensure: $Symbol \in \mathbb{C}^L$
  ϕ_{BOB}
  ϕ
  for $l = 1, \ldots, L$ **do**
    $antenna \leftarrow$ rand $\in \{1, \ldots, N\}$
    $\theta_{\text{DM}} \leftarrow$ phase$(\phi_{\text{BOB}}, antenna)$
    $\theta_n \leftarrow$ phase$(\phi, antenna)$
    $Symbol[l] \leftarrow$ QPSK$(Data[l,:])$
    $Symbol[l] \leftarrow Symbol[l] \times \exp(-i(\theta_n - \theta_{\text{DM}}))$
  end for

III. Vulnerability approach

In this section, we briefly recall the concept of vulnerability as a measure of information leakage proposed by Smith in [20] (closely related to the Bayes risk). The measure of information leakage or vulnerability—which is, in a way, the opposite of uncertainty—uses Rényi's *min-entropy* rather than Shannon entropy.

In the secure information flow analysis, the question that arises is whether a broadcast transmission could leak information about confidential data to unintended receivers. If there is indeed an information leakage, one of the main concerns is how to measure it. Intuitively, one can expect that *initial uncertainty = information leaked + remaining uncertainty*. This claim plainly suggests Shannon's traditional mutual information as the measure. However, [20] indicates that Shannon's mutual information may be inadequate to measure information leakage. A more efficient way to measure information leakage would be based on the notion of *vulnerability* and *min-entropy* [20]. We briefly revise these concepts here.

Let the triple $(\mathcal{S}, \mathcal{O}, \mathbf{C})$ represent a discrete channel. $\mathcal{S}$ is a finite set of secret input values, $\mathcal{O}$ is a finite set of observable output values, and $\mathbf{C}$ is a $|\mathcal{S}| \times |\mathcal{O}|$ channel matrix such that the element $c_{i,j}$ in the ith row and the jth column represents the conditional probability of obtaining the ith element of $\mathcal{O}$ in the output given that the input is the jth element of $\mathcal{S}$. Assuming any *a priori* probability mass function (PMF) $p_S(s)$ on $\mathcal{S}$, we have the random variable (RV) S that represents secret input values. Furthermore, taking $p_S(s)$ and $\mathbf{C}$, we can define the output RV O with a PMF given by $p_O(o) = \sum_s p_O(o|s) p_S(s)$.

Definition 1 (Vulnerability)**.** *Suppose a potential eavesdropper $\mathcal{A}$ wishes to guess the value of S in one try and, in*

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

the worst-case assumption, admit that $\mathcal{A}$ knows $p_S(s)$ and $\mathbf{C}$*; therefore, the a priori vulnerability is mathematically formulated as*

$$V(S) = \max_{s\in\mathcal{S}} p_S(s), \tag{3}$$

and the a posteriori vulnerability is given by

$$\begin{aligned} V(S|O) &= \sum_{o\in\mathcal{O}} p_O(o) \max_{s\in\mathcal{S}} p_S(s|o) \\ &= \sum_{o\in\mathcal{O}} \max_{s\in\mathcal{S}} (p_O(o|s)p_S(s)), \end{aligned} \tag{4}$$

with $0 < V(S) \le V(S|O) \le 1$.

We obtain the uncertainty measure by taking the negative logarithm of vulnerability $V(\cdot)$, i.e., Rényi's *min-entropy* [20], [21]. Thus, we have the following definitions.

Definition 2 (Initial Uncertainty)**.** *The initial uncertainty is given by*

$$H_\infty(S) = -\log_2(V(S)). \tag{5}$$

Definition 3 (Remaining Uncertainty)**.** *The remaining uncertainty is given by*

$$H_\infty(S|O) = -\log_2(V(S|O)). \tag{6}$$

Definition 4 (Information Leakage)**.** *The information leakage is given by the difference between the initial uncertainty and the remaining uncertainty. In mathematical terms, we have*

$$I_\infty(S;O) = H_\infty(S) - H_\infty(S|O) = \log_2\left(\frac{V(S|O)}{V(S)}\right). \tag{7}$$

Definition 4 reveals how vulnerable S is to one guess (in one try), given that the eavesdropper $\mathcal{A}$ knows O. On the other hand, one can assume multiple guesses for $\mathcal{A}$; hence, $I_\infty(S;O)$ might become inadequate [22]. Nevertheless, we can derive a mathematically tractable bound for at most g-guesses made by $\mathcal{A}$ as a factor of g. Namely, we have $V_g(S) \le gV(S)$ and $V_g(S|O) \le gV(S|O)$, with $V_g(S)$ being the vulnerability for g-guesses [22].

An optimal strategy is to guess the value of S according to a decreasing order of the probabilities of S—Definition 1 assumes exactly the same if only one try is allowed. Let $p_1, p_2, \ldots, p_{|\mathcal{S}|}$ be the probabilities of S such that $p_1 \ge p_2 \ge \cdots \ge p_{|\mathcal{S}|}$. Thus, the expected number of guesses required to guess S optimally, i.e., the *guessing entropy* of S, is given by

$$G(S) = \sum_{l=1}^{|\mathcal{S}|} l p_l. \tag{8}$$

Massey's guessing entropy bound in [23] establishes a lower bound on the expected number of guesses required to find S given O as a function of Shannon's conditional entropy $H(S|O)$. It claims that the guessing entropy of S given O meets

$$G(S|O) \ge 2^{H(S|O)-2} + 1. \tag{9}$$

However, this expected number of guesses may be arbitrarily large even when $H(S|O)$—and, accordingly, Massey's lower bound—is arbitrarily small. Moreover, [20] indicates through examples that $G(S)$ or $G(S|O)$ can be high even when the attacker can guess S reasonably well in one try. A similar conclusion can be drawn by assuming that p_1 and $|\mathcal{S}|$ are large enough in (8). In contrast, as the conditional min-entropy $H_\infty(S|O)$ satisfies

$$V(S|O) = 2^{-H_\infty(S|O)}, \tag{10}$$

it provides immediate security guarantees about the vulnerability of S given O since both quantities, $V(S|O)$ and $H_\infty(S|O)$, are directly related.

IV. Design

This section deals with the theoretical limits of the underlying system. In addition, we quantify the vulnerability of the proposed system and discuss optimal characteristics for the eavesdropper and an array of transmitting antennas. In what follows, Section IV-A assesses the way an eavesdropper can best obtain information from the transmitted signal, and Section IV-B discusses the design of an antenna array that minimizes the information leakage.

A. Eavesdropper

Suppose the eavesdropper $\mathcal{A}$ is in the direction ϕ_E with respect to the antenna array. It follows that the phase of the local oscillator of $\mathcal{A}$ after the handshake is given by

$$\rho_\text{LO} = \theta_\text{DM}(\phi_\text{Bob}, n_\text{R}) + \theta_{n_\text{R}}(\phi_\text{E}) + \mathbb{E}[\theta_\text{Ch}], \tag{11}$$

with $\mathbb{E}[\cdot]$ denoting the expectation operator. If the channel is additive white Gaussian noise (AWGN), then we have $\mathbb{E}[\theta_\text{Ch}] = 0$. The phase shift of symbols received by $\mathcal{A}$ after the handshake (confidential data) is given by

$$\rho_\text{S} = \theta_\text{DM}(\phi_\text{Bob}, n) + \theta_n(\phi_\text{E}) + \theta_\text{Ch}, \tag{12}$$

and the phase error in $\mathcal{A}$ can be written as

$$\begin{aligned} \rho &= \rho_\text{S} - \rho_\text{LO} \\ &= \theta_\text{DM}(\phi_\text{Bob}, n) + \theta_n(\phi_\text{E}) + \theta_\text{Ch} \\ &\quad -\theta_\text{DM}(\phi_\text{Bob}, n_\text{R}) - \theta_{n_\text{R}}(\phi_\text{E}) - \mathbb{E}[\theta_\text{Ch}]. \end{aligned} \tag{13}$$

Finally, the complex received symbol is given by

$$r = |m + w| \exp(i(\rho + \beta)), \tag{14}$$

where m represents the complex transmitted symbol with the phase β, w is a complex Gaussian RV with zero mean and variance σ^2, and $i = \sqrt{-1}$.

The eavesdropper $\mathcal{A}$ must maximize the information leakage $I_\infty(S;O)$, with S being the secret symbol whose complex representation is given by m, and O is the received symbol. Note that the mapping of S into m depends on the adopted modulation. The eavesdropper's *demodulation function* (or demodulation map) can be defined as $d : \mathbb{C} \to \mathcal{O}$; thus, the received symbol can be written as $o = d(r)$. Therefore, the task of the eavesdropper $\mathcal{A}$ is to choose a function $d(\cdot)$ that maximizes the chance of guessing S; this can be mathematically formulated as

$$\begin{aligned} &\max_{d(r)} I_\infty(S;O) \\ &\text{s.t. } |\mathcal{S}| \le |\mathcal{O}| \le |\mathcal{S}|N, \end{aligned} \tag{15}$$

or, equivalently,

$$\max_{d(r)} V(S|O) \quad \text{s.t. } |\mathcal{S}| \leq |\mathcal{O}| \leq |\mathcal{S}|N, \tag{16}$$

where the constraint $|\mathcal{S}| \leq |\mathcal{O}| \leq |\mathcal{S}|N$ is explained as follows. In fact, the totality of symbols sent through the channel by the transmitter is less than or equal to $|\mathcal{S}|N$; therefore, a set of output symbols $\mathcal{O}^*$ with $|\mathcal{O}^*| > |\mathcal{S}|N$ has spare elements. $|\mathcal{S}| \leq |\mathcal{O}|$ can be trivially understood, as the output set cannot be smaller than the input set without a loss of information in this particular context. As will become clear throughout the remainder of the paper, we commonly have $|\mathcal{O}| = |\mathcal{S}|N$.

Lemma 1. *Assume that $p_{R,S}(r,s)$ is the joint probability density function (PDF) of the complex received symbol R and the secret input values S. Let $\mathcal{P}_s$ be a complex plane such that $p_{R,S}(r,s) > p_{R,S}(r,s^*)\, \forall\, r \in \mathcal{P}_s$ and $s \neq s^*$. Then, $V(S|O)$ is maximized if and only if $d(r)$ maps all $r \in \mathcal{P}_s$ for the same observable output value o.*

Proof. Let the complex plane $\mathcal{R}$ be the sample space of R and assume that $d(r) = o \quad \forall r \in \mathcal{R}_o$ such that $\mathcal{R}_o \subset \mathcal{R}$ and $\mathcal{R}_o \cap \mathcal{R}_i = \emptyset\ \forall i \neq o$. Given the characteristics of $d(r)$, we can then write

$$p_O(o|s) = \int_{\mathcal{R}_o} p_R(r|s)\mathrm{d}r,$$

and

$$p_O(o|s)p_S(s) = \int_{\mathcal{R}_o} p_{R,S}(r,s)\mathrm{d}r.$$

Now, let s_o be the value of s which maximizes a term of the following summation

$$\sum_{o\in\mathcal{O}} \max_{s\in\mathcal{S}} (p_O(o|s)p_S(s)).$$

Thus, we can write

$$\begin{aligned}
&\max_{s\in\mathcal{S}} \left(\int_{\mathcal{R}_o} p_{R,S}(r,s)\mathrm{d}r \right) = \\
&= \int_{\mathcal{R}_o \cap \mathcal{P}_{s_o}} p_{R,S}(r,s_o)\mathrm{d}r + \int_{\mathcal{R}_o - \mathcal{P}_{s_o}} p_{R,S}(r,s_o)\mathrm{d}r \\
&\leq \sum_{a\in\mathcal{S}} \int_{\mathcal{R}_o \cap \mathcal{P}_a} p_{R,S}(r,a)\mathrm{d}r = \int_{\mathcal{R}_o} \max_{s\in\mathcal{S}} p_R(r|s)p_S(s)\mathrm{d}r.
\end{aligned}$$

It follows that

$$\sum_{o\in\mathcal{O}} \max_{s\in\mathcal{S}} (p_O(o|s)p_S(s)) \leq \int_{\mathcal{R}} \max_{s\in\mathcal{S}} p_R(r|s)p_S(s)\mathrm{d}r \tag{17}$$

with the equality condition being met only if $\mathcal{R}_o = \mathcal{P}_{s_o}\ \forall o \in \mathcal{O}$. □

Theorem 1. *Let $\mathcal{P}_{s,n}$ be a complex plane such that $p_{R,S,n}(r,s,n) > p_{R,S,n}(r,s^*,n^*)\, \forall\, r \in \mathcal{P}_{s,n}$ and $s \neq s^* \vee n \neq n^*$ with $p_{R,S,n}(r,s,n)$ being the joint PDF of the complex received symbol R, the secret input values S, and the transmitting antenna n. The eavesdropper $\mathcal{A}$ can maximize the system vulnerability by designing the demodulation function $d_{\mathcal{A}}(r)$ in such a way that for all $r \in \mathcal{P}_{s,n}$, it is mapped to the same output o.*

Proof. One can easily extend the proof of Lemma 1 by considering the secret input values with a combination of s and n as follows. Let the modulation function be $c : \mathcal{S} \times \{1, 2, \ldots, N\} \to \mathbb{C}$. Then, we can define the transmitting symbol M as an RV given by $m = c_\phi(s,n)$ for the direction ϕ. Furthermore, the sample space of M contains at most $|\mathcal{S}|N$ elements, and the PMF of M is given by $p_M(m) = p_S(s)p_n(n)$. Thus, we can apply Lemma 1 by considering M as the secret input. □

One way to interpret Theorem 1 is as follows: the vulnerability maximization for $\mathcal{A}$ refers to finding the optimal decision areas (or boundaries) for a finite output alphabet. For a practical approach, the use of Theorem 1 solely requires knowledge of the joint PDF of the complex received symbol R, the secret input values S, and the transmitting antenna n. Hereafter, we will assume that the eavesdropper has precise knowledge about $p_{R,S,n}(r,s,n)$ in order to establish the worst-case scenario regarding vulnerability. Note that any mismatch between the prior $p_{R,S,n}(r,s,n)$ at $\mathcal{A}$ and the correct $p_{R,S,n}(r,s,n)$ can lead to information leakage less than or equal to that obtained with perfect prior knowledge of $p_{R,S,n}(r,s,n)$.

One can note that $d_{\mathcal{A}}(\cdot)$ is always a noninjective surjective function. Furthermore, for a sufficiently high signal-to-noise ratio (SNR), we have a bijective function from S and n to O; therefore, the information leakage would be maximum given that $\mathcal{A}$ would be able to recover precisely S.

B. Transmitting antenna array

Here, we turn our attention to the transmitter, specifically the transmitting antenna array. In this subsection, we assess how the arrangement of transmitting antennas impacts the vulnerability of the system. Assuming the worst-case scenario (from a security viewpoint) where the eavesdropper is in its optimal operation, we provide some guidelines on the design of an antenna array that minimizes the information leakage.

Lemma 2. *For the eavesdropper $\mathcal{A}$ that uses the demodulation function $d_{\mathcal{A}}(r)$ according to Theorem 1, the vulnerability of the system is then given by*

$$V(S|O) = N - \sum_{o\in\mathcal{O}} \epsilon_{o,s_o}, \tag{18}$$

where $\epsilon_{o,s} = \Pr[d_{\mathcal{A}}(r) \neq o \cap S = s]$ is the error probability and $s_o = \arg\max_{s\in\mathcal{S}} p_O(o|s)p_S(s)$.

Proof. Let $\epsilon'_{o,s} = \Pr[d_{\mathcal{A}}(r) \neq o | S = s]$, then we have that

$$p_O(o|s) = (1 - \epsilon'_{o,s}). \tag{19}$$

Plugging (19) into (4), we obtain

$$\begin{aligned}
V(S|O) &= \sum_{o\in\mathcal{O}} (1 - \epsilon'_{o,s_o})p_S(s_o) \\
&= N - \sum_{o\in\mathcal{O}} \epsilon_{o,s_o},
\end{aligned} \tag{20}$$

with $\epsilon_{o,s_o} = \epsilon'_{o,s_o} p_S(s_o)$ and $s_o = \arg\max_{s\in\mathcal{S}} p_O(o|s)p_S(s)$. □

Lemma 2 reveals the dependence relationship between vulnerability and the error probability $\epsilon_{o,s}$. Let us now take a closer look at this error probability $\epsilon_{o,s}$, which can be expressed as

$$\epsilon_{o,s_o} = p_S(s_o)\left(1 - \sum_n \int_{\mathcal{P}_{s_o,n_o}} p_R(r|s_o,n)\mathrm{d}r\, p_n(n)\right), \quad (21)$$

with $o = d_{\mathcal{A}}(c_{\mathcal{A}}(s_o,n_o))$ and $c_{\mathcal{A}}(\cdot,\cdot)$ being the modulation function in the direction of $\mathcal{A}$ defined as $c : \mathcal{S} \times \{1,2,\ldots,N\} \to \mathbb{C}$—note that $m = c_{\mathcal{A}}(s,n)$. Because $p_R(r|s_o,n)$ is a $2\sigma^2$ variance, complex Gaussian whose center is at $c_{\mathcal{A}}(s_o,n)$, one can notice that $\lim_{\sigma\to 0} V(S|O) = 1$ and $\lim_{\sigma\to 0} I_\infty(S;O) = H_\infty(S)$. In other words, the information leakage of the system tends to its maximum value insofar as the SNR increases.

Theorem 2. *For equiprobable secret symbols and a uniformly distributed phase θ_{An} (i.e., the antenna array in conjunction with the Random Integer Generator produces a uniform phase shift), the information leakage to an eavesdropper in the direction $\phi \neq \phi_{Bob}$ is given by*

$$I_\infty(S;O) = \log_2\left(\sum_{l=1}^{L} Q_1\left(\frac{m_l}{\sigma}, \frac{r_{l-1}}{\sigma}, \frac{r_l}{\sigma}\right)\right), \quad (22)$$

with the set of nonrepeating elements in an ascending order $\{m_1, m_2, \ldots, m_L\}$ being the modules of complex symbols m, $\{r_1, r_2, \ldots, r_{L-1} | r_1 < r_2 < \cdots < r_{L-1}\}$ are the radii of the circular decision regions of the output symbols O, $r_0 = 0$, $r_L = \infty$, $Q_m(a,b) = \int_b^\infty \frac{1}{2}x\left(\exp\left(-\left(a^2+x^2\right)\right)\right)\left(\frac{x}{a}\right)^{m-1} I_{m-1}(ax)\,dx$ is the Marcum Q-function [24], and $Q_m(a,b_0,b_1) = Q_m(a,b_0) - Q_m(a,b_1)$.

Proof. Let $\theta_{An}[k]$ be the kth sample of $\theta_n(\phi)$ over time and assume that $\theta_{An}[k]$ $\forall k \in \{1,2,\ldots\}$ has a circular uniform distribution in the interval $[-\pi,\pi)$, i.e., $p_{\theta_{An}}(\theta_{An}) = 1/(2\pi)$. Because the phase error in the direction ϕ is given by $\rho = \theta_{\mathrm{DM}}(\phi_{\mathrm{Bob}},n) + \theta_n(\phi) + \theta_{\mathrm{Ch}} - \rho_{\mathrm{LO}}$ with $-\pi \le \rho < \pi$, the PDF of ρ can be obtained as

$$\begin{aligned} p_\rho(\rho) &= \sum_{\theta_{\mathrm{DM}}} \int_{-\pi}^{\pi} p_\rho(\rho|\theta_{\mathrm{DM}},\theta_{\mathrm{Ch}}) p_{\theta_{\mathrm{DM}}}(\theta_{\mathrm{DM}}) p_{\theta_{\mathrm{Ch}}}(\theta_{\mathrm{Ch}}) \mathrm{d}\theta_{\mathrm{Ch}} \\ &= \sum_{\theta_{\mathrm{DM}}} \int_{-\pi}^{\pi} \frac{1}{2\pi} p_{\theta_{\mathrm{DM}}}(\theta_{\mathrm{DM}}) p_{\theta_{\mathrm{Ch}}}(\theta_{\mathrm{Ch}}) \mathrm{d}\theta_{\mathrm{Ch}} \\ &= \frac{1}{2\pi}. \end{aligned} \quad (23)$$

Note that $p_\rho(\rho|\theta_{\mathrm{DM}},\theta_{\mathrm{Ch}})$ has a distribution identical to that of θ_n, but with the mean shifted due to the addition of $\theta_{\mathrm{DM}}(\phi_{\mathrm{Bob}},n)$, θ_{Ch}, and ρ_{LO}.

From Lemma 1, we have the boundaries of the optimal decision regions as circles. Let the radii of the decision regions be given by $\{r_1, r_2, \ldots, r_{L-1} | r_1 < r_2 < \cdots < r_{L-1}\}$, we have that

$$\begin{aligned} p_O(o = o_l|s) &= \int_{r_{l-1}}^{r_l} \frac{|r|}{\sigma^2} \exp\left(\frac{-m_l^2 - |r|^2}{2\sigma^2}\right) I_0\left(\frac{m_l|r|}{\sigma^2}\right) \mathrm{d}r \\ &= Q_1\left(\frac{m}{\sigma}, \frac{r_{l-1}}{\sigma}, \frac{r_l}{\sigma}\right), \end{aligned}$$

with $r_0 = 0$, $r_L = \infty$, and $l = \{1,2,\ldots,L-1\}$. Then, the vulnerability expression can be written as

$$V(S|O) = \frac{1}{|\mathcal{S}|} \sum_{l=1}^{L} Q_1\left(\frac{m_l}{\sigma}, \frac{r_{l-1}}{\sigma}, \frac{r_l}{\sigma}\right).$$

Finally, the information leakage is given by

$$I_\infty(S;O) = \log_2\left(\sum_{l=1}^{L} Q_1\left(\frac{m_l}{\sigma}, \frac{r_{l-1}}{\sigma}, \frac{r_l}{\sigma}\right)\right).$$

□

Corollary 1. *For equiprobable secret symbols and uniformly distributed phase $\theta_{An} = \theta_{DM}(\phi_{Bob},n) + \theta_n(\phi)$, the information leakage in the direction $\phi \neq \phi_{Bob}$ is null in phase shift key modulation.*

Proof. For the phase-shift keying modulation, we have $L = 1$ in Theorem 2. Therefore, the mutual information simplifies to

$$I_\infty(S;O) = \log_2\left(Q_1\left(\frac{m_1}{\sigma}, 0, \infty\right)\right) = \log_2(1) = 0.$$

□

Among other ways, we can understand Corollary 1 as an optimal limit for the communication security of the proposed system. Corollary 1 establishes the possibility of secure communication between the transmitter and the legitimate receiver. In other words, from the viewpoint of information leakage, Corollary 1 points to the condition that the proposed system becomes impossible to decipher. Note that an eavesdropper or a legitimate receiver in the direction ϕ_{Bob} would be able to intercept the message, even though θ_{An} follows a uniform distribution.

V. Case Study

In this section, we consider a specific arrangement of antennas in order to assess how the number of antennas and the shape of the constellation impact information leakage.

We adopt a circular antenna array, which offers a 360° field of view in the horizontal plane. If the phase centers of the antennas are evenly spread around a circle of diameter D, the phase delay can be closely approximated by [7]

$$\begin{aligned} \theta_n(\phi) &= \frac{\pi D}{\lambda} \mathrm{Re}\left(\exp\left(2\pi i\left(\frac{n}{(N+1)} + \phi\right)\right)\right) \\ &= \frac{\pi D}{\lambda} \cos\left(\frac{n}{(N+1)} + \phi\right), \end{aligned} \quad (24)$$

where λ is the wavelength, $i = \sqrt{-1}$ denotes the imaginary unit, and $\mathrm{Re}(\cdot)$ represents the real part of a complex number. In addition, we assume that the legitimate receiver is in the direction of $\phi = \pi$, i.e., $\phi_{\mathrm{Bob}} = \pi$, quadrature phase-shift keying (QPSK) modulation, $\pi D/\lambda = 1$, and n are equiprobable for all the following cases.

For *Case I* and *Case II*, we adopted two distinct demodulation processes for the eavesdropper as follows: the eavesdropper $\mathcal{A}_{\mathrm{opt}}$ adopts the demodulation function $d_{\mathcal{A}}(r)$ according to Theorem 1, and the eavesdropper $\mathcal{A}$ has the demodulation function $d_{\mathcal{A}}(r)$ like a traditional QPSK. In this way, we call $\mathrm{BER}_{\mathrm{opt}}$ the bit error rate of $\mathcal{A}_{\mathrm{opt}}$ and $\mathrm{BER}_{\mathrm{QPSK}}$ the bit error rate of $\mathcal{A}$.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

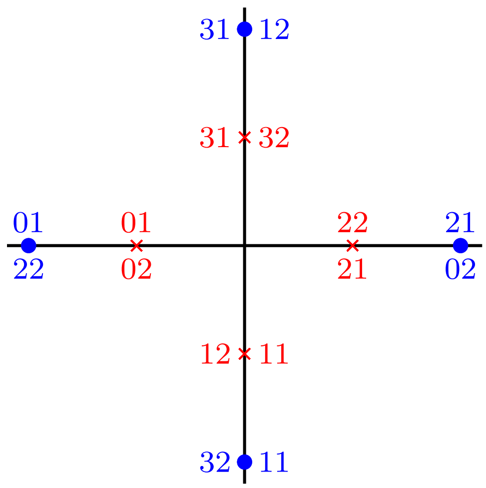

Fig. 2. Constellations on the receiver in the directions of $\phi = 60°$ (blue circles) and $\phi = 120°$ (red $\times$). The ordered pair next to the symbols is constituted by the transmitted secret symbol and the antenna used as (Sn) with $S \in \{0, 1, 2, 3\}$ and $n \in \{1, 2\}$.

A. Case I: $N = 2$

Fig. 2 depicts two constellations on the receiver. One is in the direction $\phi = 60°$, see the blue circles, and the other is in the direction $\phi = 120°$, see the red $\times$'s. We present constellations with different energy configurations for the sake of better visibility. The ordered pair next to the symbols consists of the transmitted secret symbol S and the transmitting antenna n as (Sn) with $S \in \{0, 1, 2, 3\}$ and $n \in \{1, 2\}$. For example, the ordered pair denoted by 12 means that the secret symbol S is 1, and the transmitting antenna n is 2. These two constellations were chosen because they represent extreme cases. In both constellations, the modulation process produces symbols $m = c_\phi(s, n)$ identical for different values of n. However, the symbols m that are superimposed for $\phi = 60°$ represent distinct secret symbols S while overlapping symbols m for $\phi = 120°$ represent the same secret symbol S. For instance, we have $c_{60°}(3, 2) = c_{60°}(1, 1)$ and $c_{120°}(1, 2) = c_{120°}(1, 1)$; therefore, it is impossible to decide whether the transmitted symbol is $s = 3$ or $s = 1$ for the direction $\phi = 60°$ if it receives $c_{60°}(3, 2)$, whereas an eavesdropper in the direction $\phi = 120°$ can properly recover S. This distinction can be explained as follows. An eavesdropper in the direction $\phi = 120°$ obtains two bits of information whenever it correctly estimates m, whereas another eavesdropper in the direction $\phi = 60°$ only gets one bit of information on average—the uncertainty about S is reduced by 1 bit (to two possibilities) for the direction $\phi = 60°$ given the reception of m.

Let us now introduce the AWGN such that the SNR equals 10 dB. This scenario is depicted in Fig. 3. We focus on the constellations as previously discussed: $\phi = 60°$ and $\phi = 120°$. As aforementioned, there is an information leakage of approximately 2 bits and 1 bit in the directions $\phi = 120°$ and $\phi = 60°$, respectively. However, information leakage cannot be assessed directly through the BER_{QPSK}. In other words, the BER_{QPSK} can somewhat conceal the potential vulnerability of the system. Note that although the information leakage for

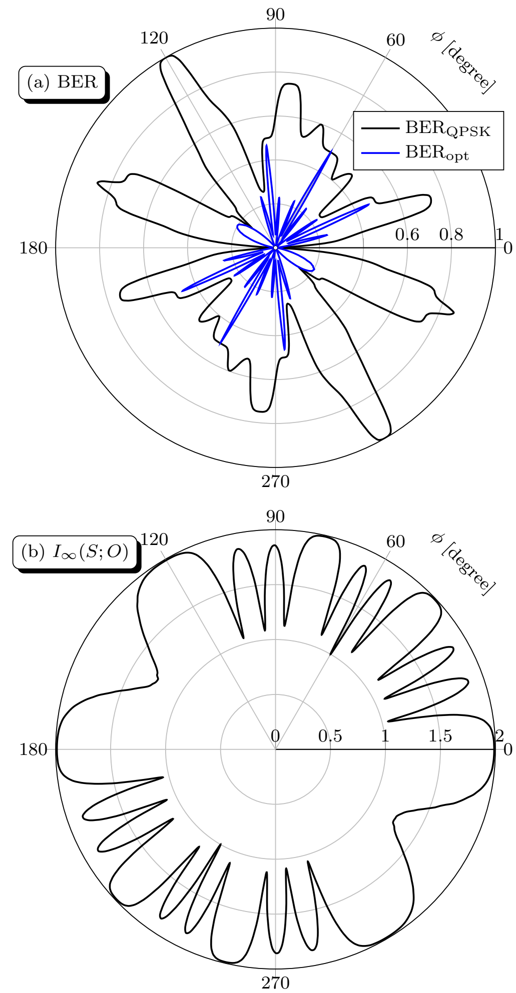

Fig. 3. BER and information leakage $I_\infty(S; O)$ versus the direction ϕ for case $N = 2$.

$\phi = 120°$ is high, the BER_{QPSK} for the case $\phi = 120°$ is also high. This counterintuitive effect can be explained as follows: the information leakage is calculated assuming that the eavesdropper applies Theorem 1, while the BER_{QPSK} calculation cannot incorporate the peculiar characteristics of the system. On the other hand, the BER_{opt} for $\phi = 120°$ is low by meeting Theorem 1, i.e., extracting the maximum information from the signal.

Fig. 3 also reveals the sensitivity (in the context of vulnerability) of the system concerning several directions. As a result, we notice the maximum information leakage for a vast set of ϕ. At best, the system provides information leakage of around 1 bit. In general terms, we can say that the system with three antennas is vulnerable to attacks. Furthermore, the BER_{opt} has values lower than the BER_{QPSK}, corroborating Theorem 1. Next, we consider larger N cases for the sake of completeness.

B. Case II: $N = 4$

Fig. 4 shows the constellation on the receiver in the direction $\phi = 10°$. For this constellation, we can say that there are four sets of four symbols each, in which the symbols are very close

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

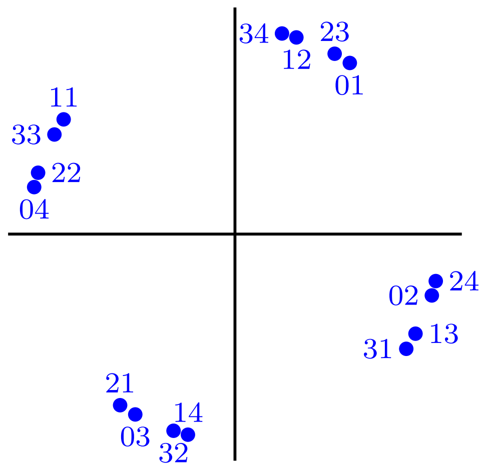

Fig. 4. Constellation on the receiver in the direction $\phi = 10°$. The ordered pair next to the symbols is constituted by the transmitted secret symbol and the antenna used as (Sn) with $S \in \{0, 1, 2, 3\}$ and $n \in \{1, 2, 3, 4\}$.

together. For example, the ordered pairs 11, 33, 22, and 04 constitute one set. For any of the four sets, it can become almost infeasible, in the presence of noise, to distinguish between the four symbols belonging to a set. Furthermore, each of the four symbols of a set comes from a different S. This characteristic of the constellation transfers little or almost no information to the receiver about the secret input S when operating under noise. Therefore, it is to be expected that it will lead to greater security for communication.

In order to verify the efficiency of the constellation shown in Fig. 4, we assume that the system is subject to an SNR of 10 dB. Fig. 5 depicts BER_{QPSK}, BER_{opt}, and information leakage for this case. Note that the information leakage is low for $\phi = 10°$. Again, the BER_{QPSK} does not satisfactorily measure the behavior of the system regarding its vulnerability. As can be seen in the figure, there is no symmetry between the BER_{QPSK} and information leakage. There is a significant reduction in the number of spikes in information leakage as N increases from 2 to 4. In addition, we obtain values below 1 for the information leakage with four antennas. The system is still somewhat vulnerable, as the information leakage is mostly above 1 bit, with a significant proportion above 1.5 bits. Lastly, we have an improvement (a decrease in BER) in the performance of the optimized eavesdropper $\mathcal{A}_{\text{opt}}$ compared with $\mathcal{A}$, corroborating Theorem 1. The following scenario discusses the case with a higher number of antennas.

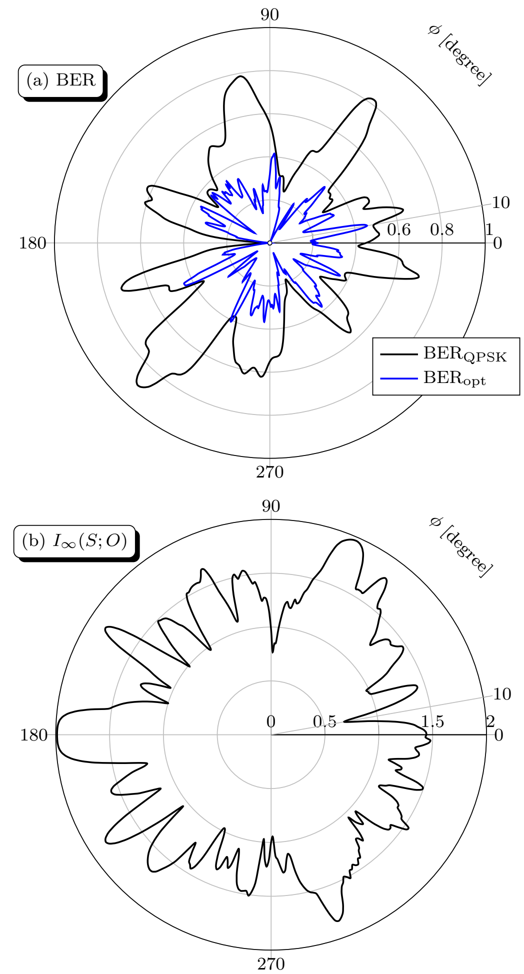

Fig. 5. BER and information leakage $I_\infty(S;O)$ versus the direction ϕ for case $N = 4$.

C. Case III: N from 14 to 300

Hereafter, the BER will be estimated considering that the receiver has properly completed the handshake and applies a trivial demodulation method. In other words, it simply demodulates the signal assuming that the modulation is the traditional QPSK. Thus, we admit a nonideal eavesdropping model. Note that the boundaries of vulnerability are assessed through information leakage measures.

Fig. 6 depicts the BER and information leakage versus the direction ϕ for different values of N at an SNR of 10 dB. Furthermore, it can be seen that the average values of the information leakage are 0.8641, 0.7733, 0.7175, and 0.6720 for $N = 14$, $N = 24$, $N = 34$, and $N = 299$, respectively. It is evident that an increase in the value of N yields a decrease in the information leakage in certain directions of ϕ. On the other hand, no significant change in BER can be observed with respect to a variation in the number of antennas. Note that although there is a substantial increase in the number of antennas from $N = 34$ to $N = 299$, we do not obtain a significant improvement with respect to the vulnerability of the system.

Fig. 7 depicts the mean of $I_\infty(S;O)$ and BER concerning ϕ for N ranging from 10 to 300. On the one hand, the system vulnerability improves dramatically with the increase in the number of antennas for $10 < N < 50$, i.e., $I_\infty(S;O)$ has a descending behavior. On the other hand, there is no significant improvement in the system vulnerability for $N > 50$. Also, in Fig. 7, it can be observed that the BER does not vary as N increases, thus, making it impossible to understand how the system vulnerability behaves as the number of antennas increases. From a practical point of view, we could say that number of antennas that would lead to the best trade-off between vulnerability and design complexity has a value close

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

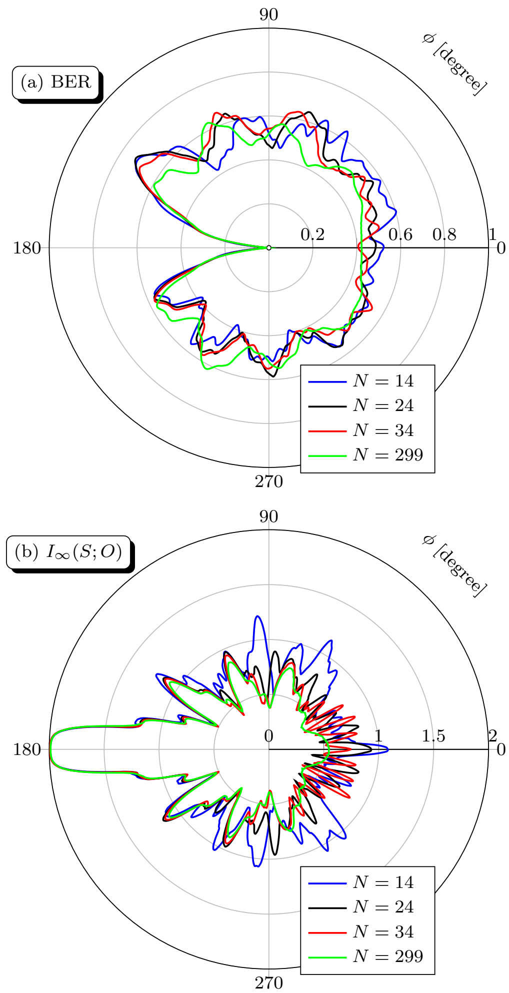

Fig. 6. BER and information leakage $I_\infty(S;O)$ versus the direction ϕ for $N = \{14, 24, 34, 299\}$. The mean values of $I_\infty(S;O)$ are 0.8641, 0.7733, 0.7175, and 0.6720 for $N = 14$, $N = 24$, $N = 34$, and $N = 299$, respectively.

to 40. For $N = 40$, the system reaches an information leakage value similar to that obtained with $N \gg 40$, while a reduction in the number of antennas to values lower than 40 sharply increases $I_\infty(S;O)$.

D. Case IV: AWGN dependence

We now turn our attention to the interdependence between information leakage and AWGN as the last case study. Unlike the case studies previously presented, the number of antennas is fixed at $N = 6$, and the SNR varies as follows: SNR $= \{9, 15, \infty\}$ dB. Fig. 8 depicts the BER and information leakage for the various SNR values. The average values for $I_\infty(S;O)$ are 1.0712, 1.4052, and 2 for SNR $= 9$ dB, SNR $= 15$ dB, and SNR $\to \infty$, respectively. As previously stated, we have a maximum information leakage in any direction in the absence of noise; in mathematical terms, $\lim_{\sigma\to 0} I_\infty(S;O) = H_\infty(S)$ and thus, $\lim_{\sigma\to 0} I_\infty(S;O) = 2$ bits for equiprobable symbols with QPSK, corroborating our theoretical deductions. Again, no significant change in the performance can be noticed through the BER for the evaluated

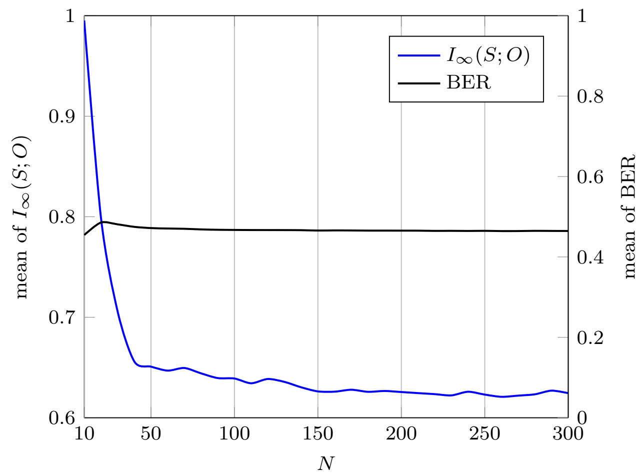

Fig. 7. Mean of information leakage $I_\infty(S;O)$ and mean of BER versus the number of antennas N.

SNR values, while the leakage information shows a clear improvement with the decrease of the SNR. Note that the leakage information reaches the maximum, and the BER tends to 1 in the direction $\phi = 260°$ for SNR $= 15$ dB. Such an effect can be understood as follows. For QPSK modulation and Gray mapping under high SNR, one can obtain BER $= 1$ by shifting the constellation so that the phase error in $\mathcal{A}$ for $\phi = 260°$ is $135° < \rho < 225° \, \forall n \in \{1, \ldots, 6\}$. However, the information leakage is not affected; the system leaks two bits of information. This case study highlights the interdependence between noise and the vulnerability of dynamic directional modulation (DDM).

Given the four previous cases, we propose the following statement.

Conjecture 1. *The closer the values of $c_\mathcal{A}(s,n) \, \forall s \in \mathcal{S}$ for the same n are, the less vulnerable the wireless system becomes.*

Conjecture 1 can be explained, among other ways, as follows. The vulnerability of a system depends on the format of the constellation generated by the DDM. In addition, constellations that coalesce symbols from the same secret input S are more vulnerable. Therefore, two design guidelines can be established: (i) given an antenna array, security can be increased in a specific direction by selecting for transmission only those antennas that meet Conjecture 1; and (ii) the antenna array design should be based on Conjecture 1.

VI. Conclusion

This paper has assessed the vulnerability of DDM by evaluating the information leakage measure, and it has also addressed the fundamental limits of said measure. Despite its usefulness as a performance metric for wireless communication systems, the proposed study has revealed the inefficiency of accessing system security (vulnerability) through the traditional demodulation method. Moreover, it is shown that an eavesdropper can remove the maximum amount of information from the transmitted signal in some directions by meeting Theorem 1 or Theorem 2. With this (optimized) eavesdropping

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

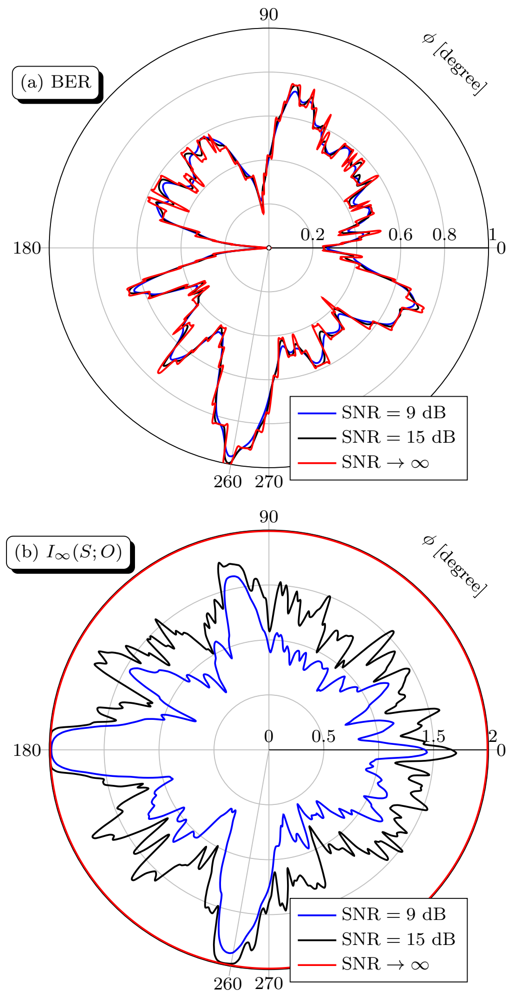

Fig. 8. BER and information leakage $I_\infty(S;O)$ versus the direction ϕ for SNR $= \{9, 15, \infty\}$ dB with $N = 6$. The mean values of $I_\infty(S;O)$ are 1.0712, 1.4052, and 2 for SNR = 9 dB, SNR = 15 dB, and SNR $\to \infty$, respectively.

model, several proposed guidelines on the design for an antenna array that minimizes the information leakage are presented. Sufficient conditions for a null information leakage in the direction $\phi \neq \phi_{\text{Bob}}$ are presented in Corollary 1. Although the proposed work provides some useful insights, it assumes an ideal eavesdropping model where the eavesdropper has perfect knowledge of the channel statistics, which is impractical in realistic models. Thus, one could investigate the impact of imperfect channel estimation on the eavesdropper performance as a possible future extension of the work presented here.

References

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[2] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, Third Quarter 2019.

[3] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit antenna selection in secure MIMO systems over α-μ fading channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, Sep. 2019.

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

[5] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, First Quarter 2017.

[6] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Second Quarter 2019.

[7] A. Narbudowicz, A. Zandamela, N. Marchetti, and M. J. Ammann, "Energy-efficient dynamic directional modulation with electrically small antennas," *IEEE Antennas Wireless Propag. Lett.*, vol. 21, no. 4, pp. 681–684, Apr. 2022.

[8] Q. Cheng, S. Wang, V. Fusco, F. Wang, J. Zhu, and C. Gu, "Physical-layer security for frequency diverse array-based directional modulation in fluctuating two-ray fading channels," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4190–4204, Jul. 2021.

[9] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[10] Y. Ding and V. F. Fusco, "Establishing metrics for assessing the performance of directional modulation systems," *IEEE Trans. Antennas Propag.*, vol. 62, no. 5, pp. 2745–2755, May 2014.

[11] A. Narbudowicz, M. J. Ammann, and D. Heberling, "Directional modulation for compact devices," *IEEE Antennas Wireless Propag. Lett.*, vol. 16, pp. 2094–2097, 2017.

[12] Y. Ding and V. Fusco, "A review of directional modulation technology," *International Journal of Microwave and Wireless Technologies*, vol. 8, no. 7, pp. 981–993, Jul. 2015.

[13] W.-Q. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1383–1396, Jul. 2018.

[14] S. Y. Nusenu, "Development of frequency modulated array antennas for millimeter-wave communications," *Wireless communications and mobile computing*, vol. 2019, pp. 1–15, 2019.

[15] T. Xie, J. Zhu, and Y. Li, "Artificial-noise-aided zero-forcing synthesis approach for secure multi-beam directional modulation," *IEEE Communications Letters*, vol. 22, no. 2, pp. 276–279, Feb. 2018.

[16] J. Parron, E. A. Cabrera-Hernandez, A. Tennant, and P. de Paco, "Multiport compact stacked patch antenna with 360° beam steering for generating dynamic directional modulation," *IEEE Antennas Wireless Propag. Lett.*, vol. 69, no. 2, pp. 1162–1167, Feb. 2021.

[17] G. Huang *et al.*, "Multicarrier directional modulation symbol synthesis using time-modulated phased arrays," *IEEE Antennas Wireless Propag. Lett.*, vol. 20, no. 4, pp. 567–571, Apr. 2021.

[18] G. Bogdan *et al.*, "Time-modulated antenna array for real-time adaptation in wideband wireless systems—part I: Design and characterization," *IEEE Trans. Antennas Propag.*, vol. 68, no. 10, pp. 6964–6972, Oct. 2020.

[19] C. Qu, K. Chen, W. Long, Y. Chen, S.-W. Qu, J. Hu, and S. Yang, "A vector modulation approach for secure communications based on 4-D antenna arrays," *IEEE Trans. Antennas Propag.*, vol. 70, no. 5, pp. 3723–3732, May 2022.

[20] G. Smith, "On the foundations of quantitative information flow," in *Foundations of Software Science and Computational Structures*, L. de Alfaro, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 288–302.

[21] A. Rényi, "On measures of entropy and information," *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability*, p. 547–561, Jan. 1961.

[22] B. Köpf and G. Smith, "Vulnerability bounds and leakage resilience of blinded cryptography under timing attacks," in *2010 23rd IEEE Computer Security Foundations Symposium*, 2010, pp. 44–56.

[23] J. Massey, "Guessing and entropy," in *Proceedings of 1994 IEEE International Symposium on Information Theory*, 1994, p. 204.

[24] W. Research, "MarcumQ," https://reference.wolfram.com/language/ref/MarcumQ.html, 2010, [version 12.2.0].

Pedro E. Góría Silva received an M.Sc. degree in Telecommunications

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3310587

from the National Telecommunications Institute (INATEL), Santa Rita do Sapucaí, MG, Brazil, and a B.Sc. degree in Telecommunication Engineering in 2020 and 2017, respectively. His research currently includes general aspects of digital transmission, semantic-functional communications, semantic-based communications, chaos-based communication, mobile communication and fading channels. He is currently working toward the Ph.D. degree at LUT University, Finland in partnership with the INATEL, Brazil.

Adam Narbudowicz received M.Sc. from Gdansk University of Technology, Poland, in 2008, Ph.D. from the Dublin Institute of Technology (now TU Dublin), Ireland, in 2013, and Habilitation from Wroclaw University of Science and Technology, Poland, in 2020. He is currently a senior researcher at Trinity College Dublin and a part-time associate professor at Wroclaw University of Science and Technology. He was twice a postdoctoral fellow of Marie Sklodowska-Curie Action co-funded projects, including a two-year research stay at RWTH Aachen University, Germany. His research interests include antenna miniaturization for IoT, physical layer security, sustainable antenna technology and the use of machine learning for radar applications.

Dr Narbudowicz has co-authored some 90 scientific publications in journals and peer-reviewed conference proceedings. He was selected as 2023 IEEE APS Young Professional Ambassador, received the Scholarship for Outstanding Young Polish Scientists in 2019, the Inaugural 2018 Prof. Tom Brazil CONNECT Excellence in Research Award, the best poster by popular vote at the 2018 IEEE-EURASIP Summer School on Signal Processing, the 3rd Best Paper Award during ISAP 2017, and the DIT Inventor Competition Award for Best Postgraduate/Staff Invention in 2012. He was also a mentor to the finalist team of the 2020 IEEE AP-S Student Design Contest. He sits on the Management Committee of the COST action SyMat, and serves as the Vice-Chair for EurAAP Small Antenna Working Group and IEEE Poland APS/MTT/AES Joint Chapter.

Nicola Marchetti is Associate Professor in Wireless Communications at Trinity College Dublin, Republic of Ireland, where he leads the Wireless Engineering and Complexity Science lab (WhyCOM). He is an IEEE Communications Society Distinguished Lecturer, an IEEE Senior Member, and a Fellow of Trinity College Dublin. He received the PhD in Wireless Communications from Aalborg University, Denmark in 2007, the MSc in Electronic Engineering from University of Ferrara, Italy in 2003, and the MSc in Mathematics from Aalborg University in 2010. He has authored more than 180 journals and conference papers, 2 books and 9 book chapters, holds 4 patents, and received 4 best paper awards. His research interests span AI for Future Networks, Bio-Inspired and Bio-Enabled Networks, Complex and Autonomous Networks, MAC Protocols and Radio Resource Management, Signal Processing for Communications, and Quantum Communications and Networks. He serves as Technical Editor for the IEEE Network Magazine, and has served as an Associate Editor for the IEEE Internet of Things Journal and the EURASIP Journal on Wireless Communications and Networking.

Pedro H. J. Nardelli received the B.S. and M.Sc. degrees in electrical engineering from the State University of Campinas, Brazil, in 2006 and 2008, respectively. In 2013, he received a double doctoral degree from University of Oulu, Finland, and State University of Campinas. He is currently Associate Professor (tenure track) in IoT in Energy Systems at LUT University, Finland, and holds a position of Academy of Finland Research Fellow. More information: https://sites.google.com/view/nardelli/

Rausley Adriano Amaral de Souza (Senior Member, IEEE) received the B.S.E.E. and M.Sc. degrees from the National Institute of Telecommunication (INATEL), Brazil, in 1994 and 2002, respectively, and the Ph.D. degree from the State University of Campinas, Campinas, Brazil, all in electrical engineering. Prior to joining the Academy, he was with industry. In 2002, he joined INATEL, where he is currently a Full Professor. His research focuses on wireless communications.

Jules M. Moualeu received the Ph.D. degree in electronic engineering from the University of KwaZulu-Natal, Durban, South Africa, in 2013. During his Ph.D. studies, he was a Visiting Scholar with Concordia University, Montreal, Canada, under the Canadian Commonwealth Scholarship Program (CCSP) offered by the Foreign Affairs and International Trade Canada (DFAIT). In 2015, he joined the Department of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, South Africa, where he is currently an Associate Professor. From 2018 to 2021, he was an Affiliate Assistant Professor with Concordia University. His current research interests include 5G and 6G enabling technologies, optical wireless communications, reconfigurable intelligent surfaces, and physical layer security in wireless networks. He received the Exemplary Reviewer Award of the IEEE COMMUNICATIONS LETTERS in 2018-2022, and the IEEE TRANSACTIONS ON COMMUNICATIONS in 2021. He served as an Associate Editor for IEEE ACCESS 2018-2023 and currently serves as an Associate Editor for Frontiers in Communications and Networks, and a Senior Reviewer for IEEE JOURNAL OF THE COMMUNICATIONS SOCIETY. He is currently the Managing Editor of IEEE COMMUNICATION LETTERS.