electronics

MDPI

Article

An Electromagnetic Analysis of Noise-Based Intrinsically Secure Communication in Wireless Systems

Marco Donald Migliore *, Daniele Pinchera, Mario Lucido, Fulvio Schettino and Gaetano Panariello

DIEI and ELEDIA@UniCAS—University of Cassino and S.L., via G. Di Biasio 43, 03043 Cassino, Italy; pinchera@unicas.it (D.P.); lucido@unicas.it (M.L.); schettino@unicas.it (F.S.); panariello@unicas.it (G.P.)
* Correspondence: mdmiglio@unicas.it; Tel.: +39-0776-299-3750

Received: 26 April 2018; Accepted: 12 July 2018; Published: 16 July 2018

Abstract: Recently there has been an increasing interest toward *unconditionally secure* communication systems in which the mechanism assuring the secrecy of the message is physical and not computational. An interesting approach proposed in the information theory literature for unconditionally secure communication is based on the use of artificial noise at a rate related to the difference between the mutual information in perfect secrecy. Since the mechanism assuring the secrecy of the message is physical and not computational, the unauthorized receiver cannot obtain information from the received signal, regardless of how much computational power is available. For this reason, such a cryptographic system is called *unconditionally secure*. The aim of this paper is to investigate an electromagnetic approach to the noise-based wireless communication systems stressing the important role of the electromagnetic propagation and antenna design. In particular, the concept of the number of degrees of freedom of the field is used to clarify the physical mechanism that allows for a decrease in the mutual information of the unauthorized channel compared to the eavesdropper channel. Numerical examples regarding both free-space propagation and rich scattering environments are shown, confirming the importance of the role of the electromagnetic propagation and antenna design.

Keywords: MIMO systems; antenna measurements; reconfigurable antenna

1. Introduction

Preventing the acquisition of critical information from unauthorized persons is a key problem in radio communications. The most advanced cryptographic algorithms are based on an approach that has been followed for more than two thousand years: an inexpensive ciphering and deciphering algorithm that requires a prohibitive amount of time and cost to be broken. This approach is called *computationally secure*. However, in spite of the complexity of the ciphering algorithms and the search for secure key sharing methods [1], all past codes have been broken, and the fast increase in computing power suggests that the most recent ones will be broken in the next future.

The final goal of cryptography is consequently the development of a cryptographic system able to resist to any cryptanalytic attack, regardless of how much computation power is available. Such a cryptographic system is called *unconditionally secure*.

In the middle of the last century, Claude Shannon showed that a ciphering system, the Vernam "one-time pad," is unbreakable [2] regardless of how much computation power is available. Successively, in a seminal paper, Wyner [3] suggested that the presence of additional noise when information is tapped from a line makes the unauthorized channel noisier than the authorized

channel. This model is known as the *degraded* channel model. He noted that the channel capacity of the authorized channel is higher than the channel capacity of the eavesdropper, and one coding strategy is able to transmit information to the authorized receiver with a vanishing block-code error probability in a completely secure way, at a rate limited by the difference between the authorized and eavesdropper channel capacity. In practice, it is possible to hide information in the additional noise affecting the eavesdropper. The great advantage of this approach is that the basic mechanism that assures the security is physical, and not algorithmical, and hence "unbreakable."

Since the paper of Wyner, and the subsequent paper of Csiszar and Korner [4], important theoretical advances have been made [5–9].

Recently, this approach has been proposed for chip-based credit, debit, and bank cards using physical unclonable function (PUF) hardware [10]. These systems take advantage of the electronic-noise-based Kirchhoff-law–Johnson-noise (KLJN) scheme to assure unconditionally secure *wired* communication.

There has recently been an impressive increase in the number of banking transactions and in the transmission of sensitive information by *wireless* systems. The aim of this paper is to analyze the noise-based communication systems in the case of wireless connection.

The research on noise-based secure communication systems is mainly carried out from an information theoretical point of view, and is focused on evaluation in different communication conditions of the *secrecy capacity*, which is defined as the maximum achievable perfect secrecy rate, where the "perfect secret rate" [3] is the amount of information that can be sent not only reliably but also confidentially. This definition parallels the classic definition of the channel capacity, which is the maximum rate assuring reliable communication. The method followed in information theory is elegant and rigorous, but suffers from the fact that it is a pure mathematical approach based on probabilistic models of communication systems. Consequently, there is still a lack of understanding of the physical mechanism at the basis of the method.

The aim of this paper is also to discuss the role of the electromagnetic propagation and antenna design in noise-based unconditionally secure communications. In this framework, an approach to obtain unconditionally secure communication based on the use of the degrees of freedom of the electromagnetic field is discussed.

The analysis followed in this paper starts from an electromagnetic point of view of the communication link. Paralleling the analysis undertaken in [11–13], it takes advantage of the concept of the number of degrees of freedom (NDF) of the electromagnetic field, defined as the minimum number of functions required to represent the field on an observation manifold within a given representation error, fixed by the noise corrupting the observed field [14].

Broadly speaking, any antenna uses the available degrees of freedom of the electromagnetic field mainly following two possible goals: to concentrate (and possibly maximize) energy on the receiving antenna or to maximize the amount of information available on the receiving antenna [11,15–17]. In this paper, it will be shown that, in the noise-based unconditionally secure communication systems, the degrees of freedom of the electromagnetic field are used in a *third way*. Signal *and* noise are transmitted at the same time using a strategy that avoids any increase in noise at the "authorized" receiver taking advantage of the degrees of freedom that are not used to transmit information. In this way, the noise at the unauthorized receiver is increased without affecting the noise at the authorized receiver. This causes a decrease in the channel capacity of the unauthorized receiver compared to the authorized receiver, which can transmit information buried in the additional noise affecting the eavesdropper.

This paper offers a theoretical electromagnetic analysis of the problem, which can be easily extended to consider near-field communications. Accordingly, the possible applications of the techniques are quite large, and covers contactless payments, cryptographic key exchange, and in general wireless exchange of highly sensible data.

2. Degrees of Freedom of the Electromagnetic Field in Noise-Based Unconditional Security

Following a widely adopted convention in literature, in this paper, the transmitter will be called Alice, the legitimate receiver will be called Bob, and the eavesdropper will be called Eve.

Let us consider the continuous communication channel model drawn in Figure 1 [11,12,16,17]. For the sake of simplicity, a scalar case will be considered. Alice's transmitting antenna is modeled as a current source $J(r')$, $r' \in D$, where D is the the domain in which the current source is placed. Bob's antenna is placed in the domain D_1 bounded by the surface Ω_A, while Eve's antenna is placed in the domain D_2 bounded by the surface Ω_U, where D_1, D_2 and D are not intersecting domains. Considering for sake of simplicity a scalar problem, the field on Bob's antenna domain is:

$$E(r) = \int_D G(r, r')J(r')dr' \quad r \in D_1 \tag{1}$$

where G is Green's functions (evaluated in the presence of scattering objects if they are present in the environment).

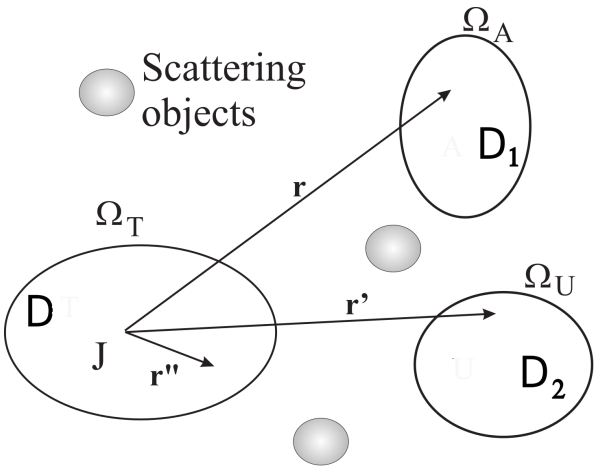

Figure 1. Geometry of the problem; D = Alice's antenna domain; D_1 = Bob's antenna domain; D_2 = Eve's antenna domain.

Paralleling the approach followed in [11] and considering fields and currents as elements in the L_2 Hilbert space equipped with the standard norm, the radiation operator in Equation (1) is expanded using the Hilbert–Smidth decomposition, obtaining

$$E = \sum_{i=1}^{\infty} \sigma_i < J, v_i > u_i \tag{2}$$

where $< \cdot, \cdot >$ denotes the inner product, and (u_i, v_i, σ_i) is the singular systems of the operators G [11].

The presence of thermal noise and uncertainties in the receiver limits the accuracy level at which the field can be observed. The number of singular functions required to represent the field at a given level of accuracy (that is fixed by the receiver noise and uncertainty level) fixes the NDF of the field observed on the D_1, which will be denoted as NDF (a more rigorous definition in terms of $n-$widths is reported in [12,14]) (In practice, the NDF of the field is the number of effective dimensions of the radiation operator in Equation (1). The NDF depends on the electrical dimensions and shape of the source and on the dimension and shape of the surface on which the radiated field is observed. In the case of the observation surface completely surrounding the source, the NDF is approximately double the length of the radiating system measured in wavelengths in the case of linear antennas, and one quarter of the area of the antenna in the case of surface radiating systems [14]. An increase in the dimension of the radiating system causes an increase in the NDF of the field.).

As shown in [12], the first NDF components $J_i = < J, v_i >$ of the source current can potentially transmit statistically independent information toward D_1, while the other components excite a field that is negligible on D_1 since it is covered by the thermal noise. The energy radiated on D_1 is proportional to the singular values σ_i of the field configuration u_i. Each spatial configuration of the field can transmit statistically independent information [12].

However, small values of σ_i indicates that the amount of energy radiated on D_1 is negligible. Consequently, excitation of configurations of the field associated to low singular values gives configurations of the field that do not significantly contribute to Bob's receiving domain. These spatial channels cannot be used to transmit information to Bob but can be used to send noise without significantly affecting Bob's receiver.

In order to clarify these concepts, let us consider a simple two-dimensional example, consisting of a circular source (representing Alice's antenna) having a radius $a = 2\lambda$ and an observation domain consisting of a $\pi/8$ long arch of circle (representing Bob's antenna) concentric to the source and having radius $R = 100\lambda$.

The Hilbert–Smith decomposition can be obtained analytically using cylindrical wave expansion (it is understood that, in more complex cases, it is possible to estimate the singular system discretizing the source and the observation curve. In this way, the operator is approximated by a matrix, whose singular system can be obtained using the singular value decomposition algorithm) [12].

The singular values of this electromagnetic system normalized to σ_1 are plotted in Figure 2. The analysis of the figure gives a clear picture of the possibilities of the communication systems associated with the electromagnetic model.

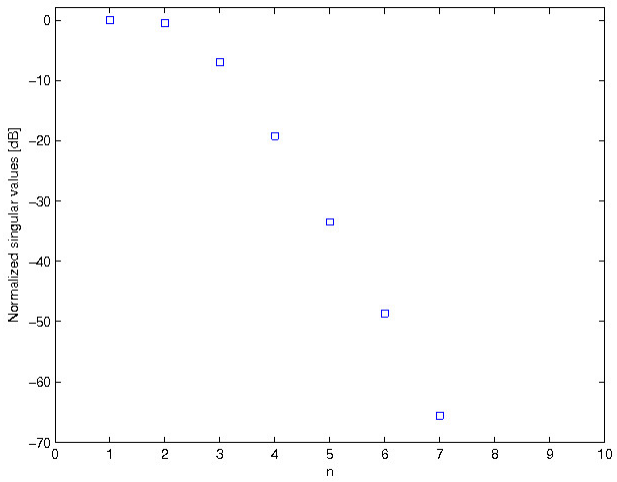

Figure 2. Singular values [dB].

First of all, we can note two singular values at practically the same level. Excitations related to these two singular values (i.e., v_1 and v_2) can be associated to statistically independent information, i.e., to two different MIMO channels. The amplitudes of the field radiated by v_1 and v_2 (called also singular modes) are plotted, respectively, in Figure 3a,b.

The other singular values are lower and indicate a less effective capacity to transmit energy on the observation arch D_1. As an example, in Figure 3c, the amplitude of the field configurations associated with the 5th singular value is plotted, showing a low value of the field on the observation arch. On the contrary, the energy is concentrated just outside the observation arch. In particular, the ratio between the energy concentrated on the observation arch by the n-th and the m-th mode is given by the σ_n^2/σ_m^2. Consequently, if we send information transmitting P_s power on the n-th singular mode and noise transmitting P_i power on the m-th singular mode, we have a signal/interference ratio

on the observation arch of $P_s\sigma_n^2/(P_i\sigma_m^2)$. In Figure 3d, the normalized currents associated to the 1st singular mode (solid curve), 2nd singular mode (dashed curve), and 5th singular mode (dotted curve) are also plotted, showing an acceptable dynamic range.

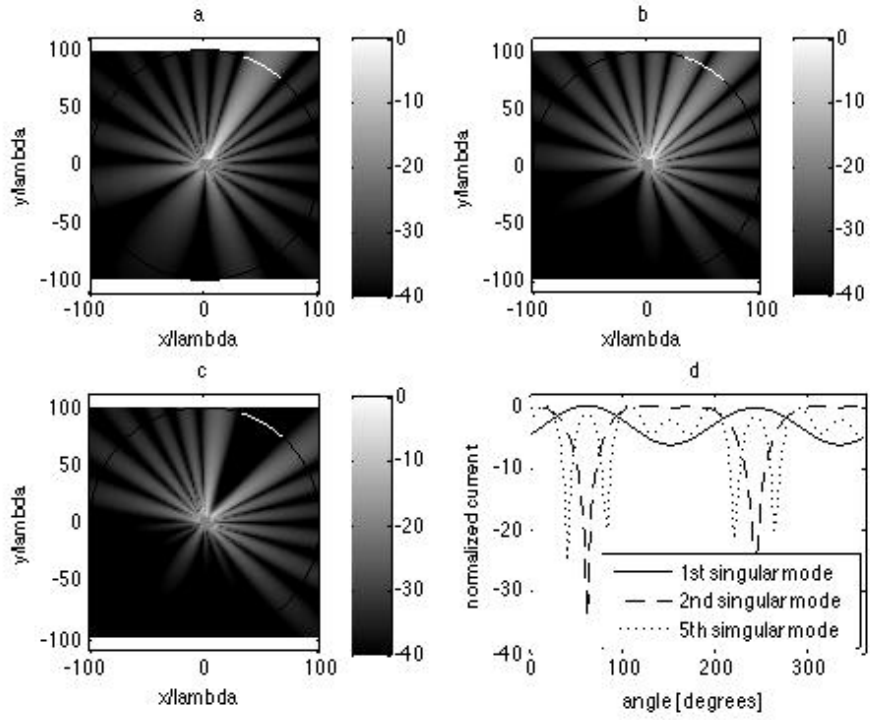

Figure 3. Singular mode field amplitude and currents; in (**a**–**c**) the circle having $R = 100\lambda$ radius is plotted as a black curve (barely visible); the observation arch is plotted as white curve (**a**) 1st singular mode amplitude; (**b**) 2nd singular mode amplitude; (**c**) 5th singular mode amplitude; (**d**) normalized singular mode currents, solid line: 1st, dashed line: 2nd mode, dotted line: 5th mode .

In order to clarify this concept, in Figure 4a, the SNR in case of signal transmitted on the first singular mode and -60 dB Gaussian noise are plotted, while in Figure 4b, the SNRI (signal-to-noise-plus-interference ratio) in the case of noise transmitted on the fifth singular mode with $P_i/P_s = 10$ is shown. The use of the fifth singular mode allows for a decrease in the SNRI everywhere except in the exact area covered by the observation arch.

In Figure 4c,d, the same data when the second singular mode is used to send information are plotted.

Each communication channel transmits an amount of information given by the mutual information

$$I(x,y) = \sum_{k=1}^{N} \log_2 (1 + SNRI_k) \qquad \text{[bits/s/Hz]} \tag{3}$$

where $SNRI_k$ is the SNRI at the receiver of the k-th communication channel. In our case, if we use two channels (associated to v_1 and v_2), then $N = 2$. Figure 4 clearly shows that an eavesdropper in an angular direction different form the angular direction of Bob's arch suffers from a high $SNRI$ and hence the mutual information between the eavesdropper (Eve) and Bob is much lower than the mutual information between Alice and Bob.

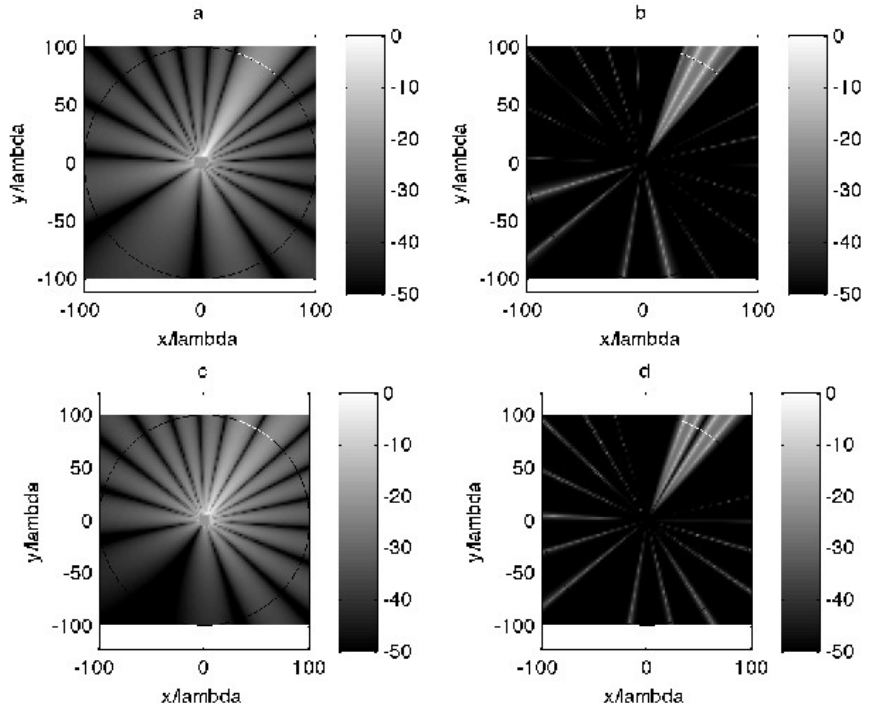

Figure 4. SNR; (**a**) the first mode with only thermal noise (−60 dB); (**b**) the first mode with thermal noise and artificial noise on the 5th singular mode; (**c**) the second mode with only thermal noise (−60 dB); (**d**) the second mode with thermal noise and artificial noise on the 5th singular mode.

Coming back to the point of view of information theory, as discussed in the introduction, a metric able to evaluate the performance of the secret communication system is the secret capacity. However, the precise value of the secret capacity is not easy to evaluate, and a widely adopted surrogate is the difference between the mutual information of the legitimate channel $I(\mathbf{x}, \mathbf{y})$ and of the eavesdropper $I(\mathbf{x}, \mathbf{z})$ [4,18,19]:

$$\Delta I = [I(\mathbf{x}, \mathbf{y}) - I(\mathbf{x}, \mathbf{z})]^+ \tag{4}$$

where $[x]^+ = \max[x, 0]$. This quantity is a lower bound of the secret capacity in Gaussian channels [3] and allows for a simple linkage between the electromagnetic analysis undertaken in this paper and the approach followed in information theory. In particular, the use of artificial noise allows for an increase in the secret capacity of a communication system.

Finally, it is understood that the above described electromagnetic approach can be followed in a no-free-space condition, considering the proper Green's function.

3. Numerical Examples

In the following examples, we suppose that Alice knows the angular position of Bob. The radiating elements of Bob's, Alice's, and Eve's antennas consist of short dipoles $l = \lambda/5$ long.

The first example regards an antenna radiating in a free-space condition. The antenna consists in 7 short wire antennas having $l = \lambda/5$ length. With reference to Figure 5a, the dipoles 1 and 2, placed along $\hat{y}$ and $\hat{z}$ axis, transmit "useful" information, while the dipoles 3, 4, 5, 6, and 7 transmit interference noise according to the following strategy. The noise signal transmitted by 3 and 4 are completely correlated—4 if fed by the opposite of the noise signal feeding 3 (e.g., the signals have a π phase difference). Moreover, the noise signal transmitted by 5 and 6 are completely correlated—5 if fed by the opposite of the noise signal feeding 6. The noise signals feeding 3 is completely uncorrelated

from the noise signal feeding 5. Finally, the noise signal transmitted by 7 is completely uncorrelated from all other transmitted noise. The above strategy assures that interference noise does not reach Bob.

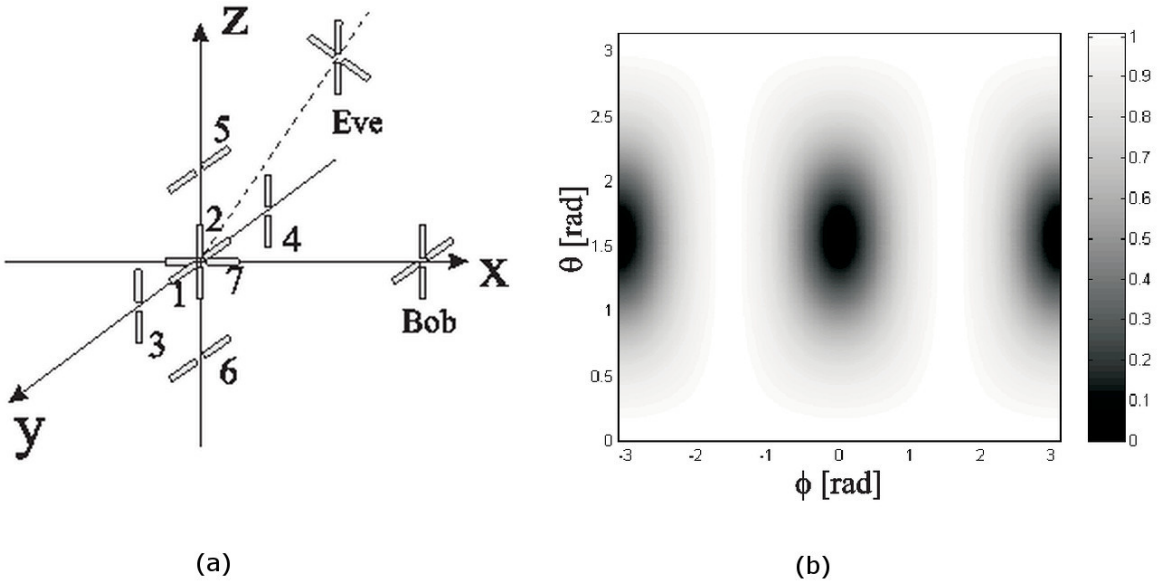

Figure 5. Geometry of the problem; Alice's antenna consists of 7 short dipoles; (**a**) geometry of the problem; (**b**) ΔI [bits/s/Hz], 7 TX dipoles, P_s = 15 W, P_i = 15 W.

In the numerical simulation, P_t = 30 W, P_s = 15 W, and the average SNR ratio at the receivers is equal to 12 dB. The dipoles (1 and 2) are fed with 7.5 W each, the dipole 7 is fed with 15/3 W, and the remaining four elements are each fed with 15/6 W. In Figure 5b, the difference between the mutual information, ΔI, is plotted in gray scale in the case of Eve's antenna placed on the sphere where radius R = 10,000 λ. The plot shows that the mutual information quickly drops in directions different from that of Bob's antenna ($\theta = \pi/2$, $\phi = 0$).

As a second example, we consider secure communication in complex environments, such as an urban area, i.e., in the presence of a large number of scattering objects. The propagation phenomenon between Alice and Bob is described by the channel matrices $\mathbf{H}_s$ and $\mathbf{H}_i$, whose effective ranks are upper-bounded by the degrees of freedom of the field [11]. In the following example, Alice's antenna consists of $M_s = 4$ elements radiating "useful" information, placed in $x = (-1.5, -0.5, 0.5, 1.5)\lambda$ along the $\hat{x}$ axis, and $M_i = 7$ elements radiating interference noise, placed at $x = (-2.5, -2, -1, 0, 1, 2, 2.5)\lambda$ along the $\hat{x}$ axis. Bob's antenna consists of four elements placed at $x = (-1.5, -0.5, 0.5, 1.5)\lambda$, $y = (40, 40, 40, 40)\lambda$. Eve's antenna consists of four elements placed in $x = ([-1.5, -0.5, 0.5, 1.5]\lambda + x_0\lambda)$, $y = (y_0, y_0, y_0, y_0)\lambda$, where $4\lambda \leq x_0 \leq 45\lambda$ and $-20\lambda \leq y_0 \leq 20\lambda$. The elements of all the antennas are short wires $\lambda/5$ long, with an axis along the $\hat{z}$ axis. The total average transmitted power is 11 W (4 W equidistributed among the four elements radiating "useful" information, and 7 W equidistributed among the seven elements transmitting interference noise.) The average signal/noise ratio at each element of Bob's antenna is 26 dB. One hundred fifty different environments, each of them consisting of 40 scattering objects placed at random positions, are considered. For each position (x_0, y_0) of Eve's antenna, the average value of ΔI is calculated [20]. This value will be indicated as $\bar{\Delta I}$. The optimal distribution of the available power between noise and signal is to be obtained by numerical optimization. The result is shown in Figure 6 ($\bar{\Delta I}$ [bits/s/Hz]). The contour plot shows that perfect secret communication is possible also when Eve's antenna is close to Alice's antenna.

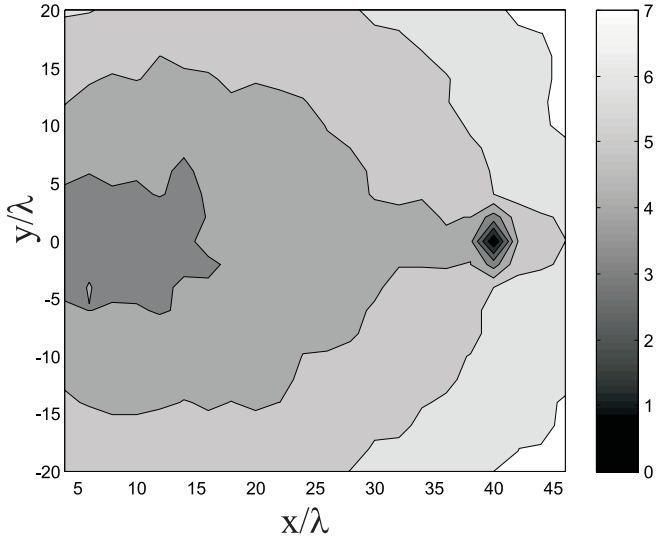

Figure 6. $\bar{\Delta I}$ [bits/s/Hz], $P_s = 4$ W, $P_i = 7$ W.

4. Conclusions

The aim of this paper is to discuss the problem of noise-based unconditional security from an electromagnetic point of view.

The physical mechanism at the basis of the secret communication is explained by means of the degrees of freedom of the field, which are able to convey information and noise in spatially orthogonal channels. In this way, it is possible to increase the noise at the eavesdropper without affecting the noise at the legitimate receiver. According to some fundamental results of information theory, it is possible to hide information in the additional noise affecting the eavesdropper.

The simple examples shown in this paper confirm the role of antenna design and suggest including secret communication models in a genetic algorithm in order to find the optimal configuration of Alice's and Bob's antenna in a given scenario. This analysis will be object of future investigations.

As a final observation, in order to make the channel secure, a non-negligible percentage of the available power is radiated as artificial noise. Loosely speaking, the allocation of power to noise causes a decrease in the channel capacity of the system that follows logarithmic law. This is the cost that must be paid to cover information into artificial noise. The optimal distribution of available power between signal and noise is a further problem that will be the object of future investigations.

Author Contributions: Data curation, M.L.; Formal analysis, F.S. and G.P.; Investigation, D.P.; Methodology, M.D.M.

Funding: This paper has been partially supported by the MIUR program 'Dipartimenti di Eccellenza 2018- 2022' .

Conflicts of Interest: The authors declare no conflict of interest

References

1. Pinchera, D.; Migliore, M.D. Effectively Exploiting Parasitic Arrays for Secret Key Sharing. *IEEE Trans. Veh. Technol.* **2016**, *65*, 123–131. [CrossRef]
2. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
3. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
4. Csiszar, I.; Korner, J. Broadcast channel with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
5. Lai, L.; Gamal, H.E.L.; Poor, H.V. The Wiretap Channel With Feedback: Encryption Over the Channel. *IEEE Trans. Inf. Theory* **2008** *54*, 5059–5067. [CrossRef]
6. Cho, A. Simple noise may stymie spies without quantum weirdness. *Science* **2005**, *309*, 2148. [CrossRef] [PubMed]

7. Palmer, D.J. Noise encryption keeps spooks out of the loop. *New Sci.* **2007**, *2605*, 32. [CrossRef]
8. Vuppala, S.; Biswas, S.; Ratnarajah, T. Secrecy Outage Analysis of k th Best Link in Random Wireless Networks. *IEEE Trans. Commun.* **2017**, *65*, 4478–4491. [CrossRef]
9. Javan, M.R.; Sheikhzadeh, S.; Mokari, N. Secure communications in OFDMA decode and forward relay assisted networks in presence of multiple eavesdroppers. In Proceedings of the 2016 8th International Symposium on Telecommunications (IST), Tehran, Iran, 27–28 September 2016; pp. 134–138.
10. Kish, L.; Entesari, K.; Granqvist, C.; Kwan, C. Unconditionally Secure Credit/Debit Card Chip Scheme and Physical Unclonable Function. *Fluct. Noise Lett.* **2016**, *16*, 1750002. [CrossRef]
11. Migliore, M.D. On the Role of the Number of Degrees of Freedom of the Field in MIMO Channel. *IEEE Trans. Antennas Propag.* **2006**, *54*, 620–628 [CrossRef]
12. Migliore, M.D. On Electromagnetics and Information Theory. *IEEE Trans. Antennas Propag.* **2008**, *56*, 3188–3200. [CrossRef]
13. Migliore, M.D. On the Sampling of the Electromagnetic Field Radiated by Sparse Sources. *IEEE Trans. Antennas Propag.* **2015**, *63*, 553–564. [CrossRef]
14. Bucci, O.M.; Franceschetti, G. On the degrees of freedom of scattered fields. *IEEE Trans. Antennas Propag.* **1989**, *37*, 918–926. [CrossRef]
15. Jensen M.A.; Wallace, J.A. Review of Antennas and Propagation for MIMO Wireless Communications. *IEEE Trans. Antennas Propag.* **2004**, *52*, 2810–2824. [CrossRef]
16. Jensen, M.A.; Wallace, J.W. Capacity of the Continuous-Space Electromagnetic Channel. *IEEE Trans. Antennas Propag.* **2008**, *56*, 524–531. [CrossRef]
17. Gruber, F.K.; Marengo, E.A. New Aspects of Electromagnetic Information Theory for Wireless and Antenna Systems. *IEEE Trans. Antennas Propag.* **2008**, *56*, 3470–3484 . [CrossRef]
18. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
19. Li, Z.; Trappe, W.; Yates, R. Secret Communication via Multi-antenna Transmission. In Proceedings of the 41th Conference on Information, Sciences and Systems, Baltimore, MD, USA, 14–16 March 2007.
20. Cover, T.M.; Thomas, J.A. *Information Theory*; John Wiley & Sons: Hoboken, NJ, USA, 1991.