A New Metric for Measuring the Security of an Environment: The Secrecy Pressure

A New Metric for Measuring the Security of an Environment: The Secrecy Pressure

Lorenzo Mucchi, *Senior Member, IEEE*, Luca Ronga, *Senior Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, Kaibin Huang, *Senior Member, IEEE*, Yifan Chen, *Senior Member, IEEE*, and Rui Wang

***Abstract*— Information-theoretical approaches can ensure security, regardless of the computational power of the attackers. Requirements for the application of this theory are: 1) assuring an advantage over the eavesdropper quality of reception and 2) knowing where the eavesdropper is. The traditional metrics are the secrecy capacity or outage, which are both related to the quality of the legitimate link against the eavesdropper link. Our goal is to define a new metric, which is the characteristic of the security of the surface/environment where the legitimate link is immersed, regardless of the position of the eavesdropping node. The contribution of this paper is twofold: 1) a general framework for the derivation of the secrecy capacity of a surface, which considers all the parameters that influence the secrecy capacity and 2) the definition of a new metric to measure the secrecy of a surface: the secrecy pressure. The metric can be also visualized as a secrecy map, analogously to weather forecast. Different application scenarios are shown: from "forbidden zone" to Gaussian mobility model for the eavesdropper. Moreover, the secrecy outage probability of a surface is derived. This additional metric can measure, which is the secrecy rate supportable by the specific environment.**

***Index Terms*— Physical-layer security, secrecy pressure, secrecy capacity, secrecy outage, security of wireless communications.**

I. Introduction

IN WIRELESS networks, transmission between legitimate nodes can easily be intercepted by an eavesdropper due to the broadcast nature of the wireless medium. This makes wireless transmissions highly vulnerable to eavesdropping attacks. Existing communications systems typically adopt cryptographic techniques in order to achieve confidential transmission, to prevent an eavesdropper from interpreting data transmission between legitimate users.

It is known that encrypted transmission is not perfectly secure, since the cipher text can still be decrypted by an eavesdropper through a brute-force attack, an exhaustive search of the encryption key into the cipher text.

To this end, physical-layer security is an emerging alternative paradigm to protect wireless communications against eavesdropping attacks, including brute-force attacks. In fact, the security of cryptographic techniques is implicitly set into the practical assumption that the attacker does not have enough computational power to hack the cipher text in a reasonable amount of time. Thus, security of encryption algorithm cannot be measured exactly. On the contrary, information-theoretical physical-layer security does not need to make any assumption of the computational power of the attacker, and, in addition, the security of a communication link can be exactly measured.

Physical-layer security work was pioneered by Shannon and evolved by Wyner in [1], where a discrete memoryless wiretap channel was examined for secure communications in the presence of an eavesdropper. Perfectly secure data transmission can be achieved if the channel capacity of the legitimate link is higher than the eavesdropper link (from source to eavesdropper). In [2], Wyners results were extended to Gaussian wiretap channel: a new metric, the secrecy capacity, was proposed. The secrecy capacity was derived as the difference between the channel capacity of the legitimate link and of the eavesdropper link. If the secrecy capacity is above zero, the legitimate source can adapt the data rate in order to let the destination decode the information, while the data overheard by the eavesdropper is too few and noisy to be decoded. If the secrecy capacity falls below zero, the transmission from source to destination becomes completely insecure, and the eavesdropper can succeed in interpreting the data. In order to improve the security against eavesdropping attacks, one solution is to reduce the probability of occurrence of an intercept event through enlarging the secrecy capacity.

As a consequence, there are extensive works aimed at increasing the secrecy capacity of wireless communications by exploiting multiple antennas [3] and/or cooperative relays [4].

A. Related Works

There are some examples in literature of papers attempting to create a physical region to face the randomness of the

Manuscript received September 12, 2016; revised January 20, 2017; accepted February 28, 2017. The work of X. Zhou was supported by the Australian Research Council's Discovery Projects under Grant DP150103905. The work of Y. Chen was supported by the Guangdong Natural Science Funds under Grant 2016A030313640. The associate editor coordinating the review of this paper and approving it for publication was M. Elkashlan.

L. Mucchi is with the Department of Information Engineering, University of Florence, I-50139 Firenze, Italy (e-mail: lorenzo.mucchi@unifi.it).

L. Ronga is with the National Inter-universities Consortium on Telecommunications, University of Firenze research Unit, I-50139 Firenze, Italy (e-mail: luca.ronga@cnit.it).

X. Zhou is with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

K. Huang is with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong (e-mail: huangkb@ieee.org).

Y. Chen is with the Faculty of Science and Engineering, The University of Waikato, Hamilton 3240, New Zealand, also with the Faculty of Computing and Mathematical Sciences, The University of Waikato, Hamilton 3240, New Zealand, and also with the Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen 518055, China (e-mail: yifan.chen@waikato.ac.nz).

R. Wang is with the Department of Electrical and Electronic Engineering, South University of Science and Technology of China, Shenzhen 518055, China (e-mail: wang.r@sustc.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2017.2682245

eavesdropper location and/or the amplitude fluctuation due to fading. All these attempts are basically based on the use of multiple antennas and beamforming [5], [10]–[12]. These works aim at building a region as small as possible where the message can be considered secure. The region is built by using beamforming and/or antenna coding between the legitimate transmitter and receiver, or with the help of friendly surrounding nodes (artificial noise injection, jamming). Actually, the definition of the physical region can differ from paper to paper, but mainly beamforming or jamming are used in the works based on information-theoretical parameters, in the form of antenna arrays [10] or distributed antennas [5].

In [6] secrecy rate maximization and power consumption minimization for a multiple-inputmultiple-output (MIMO) secrecy channel is investigated. A multiantenna cooperative jammer is employed to improve secret communication in the presence of a multiantenna eavesdropper. In [7] and [8] a phase-shifting array is used to produce security in a given direction (directional modulation). The resulting signal is direction-dependent and thus the signal can be purposely distorted in other directions but the desired one. This approach can be used to enhance the security of multiuser multi-input multiple output (MIMO) communication systems when a multiantenna eavesdropper is present [9].

The metric used to measure the security of the legitimate link is always the received signal to noise plus interference ratio (SINR) or the secrecy outage. The metric, such as the secrecy outage, is well known in literature and it is related to the quality of the legitimate link, given the position of transmitter and receiver, the transmit parameters (power, coding, beamforming, etc.), as well as the location of eavesdropping nodes and interference sources. Other papers based on information-theoretical security typically use the metrics such as secrecy capacity or secrecy outage to measure the security level of the legitimate link by supposing to know the positions and the channel state information of the eavesdroppers and interferers. In order to drop out the dependance on the positions of the eavesdropping or interference nodes,[1] a more general secrecy metric which is basically a characteristic of the network topology can be reached by averaging out the secrecy capacity over all the possible positions of eavesdroppers or interferers [13], [14]. Anyway, all the above mentioned papers deal with metrics which express a characteristic of the link, not of the surface where the link is immersed.

B. Our Contribution

The secrecy capacity is a good metric to evaluate how much is secure a single communication link. But in many practical scenarios a metric which is related to the specific environment can be more effective. For this reason we propose and test here a new metric which bonds the secrecy to the surface of the environment. We named this metric *secrecy pressure*, taking an analogy from the weather forecasting. The secrecy pressure is defined as the secrecy capacity insisting over the infinitesimal element of the surface. This metric can be used for several practical scopes: from deriving the secrecy of a specific surface/environment, to calculate which is the optimum transmitting antenna orientation or friendly jammer position.

Differently from traditional metrics such as the conventional secrecy capacity, our metric does not imply to know where Eve is. To be more clear, in our approach the secrecy capacity is calculated for each point (x, y) of a surface S. To do this we suppose that Eve is located in (x, y). Then, we integrate over x and y along the surface S, thus eliminating the dependence on the position of the eavesdropper. The integration operation is, de facto, as taking the average over the space (instead of time). The resulting metric is the secrecy capacity than the entire surface S has got. We call this metric secrecy pressure since it tells how much security insists over a surface S. In other words, we calculate how much secure is an environment, given the position of Alice, Bob and (if present) interferers. It is more practical because 1) we do not have to make any assumptions on the position of the eavesdropper; 2) the new metric is a property of the environment, and not of the point where Eve is located; 3) we calculate a number which gives an insight on how much secure is the environment were going to transmit. The closest concept to this new metric is the network secrecy developed by M. Win *et al.* [13]. The network secrecy is a metric which evaluates the secrecy of an entire network of nodes (not an environment). Legitimate nodes and eavesdropping nodes are randomly distributed as Poisson point processes (PPP). The secrecy capacity is calculated for each legitimate link, given the position of the eavesdroppers. The dependence on the eavesdroppers positions is dropped by averaging out respect to all possible realization of the PPP distribution of the eavesdropper nodes.

The paper also includes a general framework which evaluates the secrecy capacity over a surface. The framework describes all the parameters affecting the secrecy capacity: spatial distribution of the nodes (legitimate and interfering) on a surface, antennas' orientations and patterns, path loss and fast fading statistics of the communication links, transmitting powers. No hypothesis is made over the position of the eavesdroppers, the metric is calculated over the entire surface, as the eavesdropper could be in each point of the surface. Static as well as statistical mobility model are supposed for the eavesdropper. The results show how the metric can be useful in giving an immediate insight on the leakage zones in the surface, and how to adjust the parameters in order to maximize the secrecy. The optimization problem is here formulated for the transmitting antenna orientation and for the position of a friendly jammer.

It is important to highlight that the secrecy pressure does not need to know the position of the eavesdropper (Eve) on the surface of interest. Typically the papers in literature assume to know the position of Eve, which is usually an unpractical assumption. The secrecy pressure or the secrecy map parameters are calculated by assuming that Eve can stay in each point of the surface. If no information about eavesdropper is known, it could be located in any point of the surface with equal probability. We did not introduce a PPP distribution of eavesdropping nodes, although this is a

[1]The eavesdroppers and interferers are supposed to be spatially distributed around the legitimate link with a point poisson process (PPP) distribution.

common approach, since we suppose that Eve can stay in each point of the surface. Typically, the PPP distribution is used to calculate how many eavesdroppers are within the range of the legitimate transmitter, and than average out the secrecy capacity. Our approach is different, we are interested in a new metric which is a characteristic of the surface. Anyway, a PPP distribution for the presence of Eve over the surface can be easily assumed in our case too. The secrecy pressure contains all the parameters that can cause a variation of the secrecy capacity, and thus it can be optimized respect to many (known) parameters (transmit antenna orientation, interference node positions or powers, etc.), separately or jointly.

Another known metric in information-theoretical physical-layer security is the secrecy outage, i.e., the probability that the secrecy capacity is below a target rate. We have derived here the secrecy outage probability of a surface (SOPS). In this case we have supposed that the presence of Eve on the surface is not perfectly known, but it has an uncertain which we have modelled as a Gaussian distribution.

The instant fading coefficient of Eve's channel should be anyway known or estimated in order to derive the secrecy pressure instant by instant. This estimation can be relaxed if the evaluation of the secrecy pressure is done in ergodic channel. The ergodic secrecy pressure can be a useful tool in many practical applications.

Practical applications of the propose metric could be tactical communications: a scenario in which the transmission cannot surely be overheard in a particular zone of the surface. Another scenario could be when the information cannot be leaked along a specific path or street, where the eavesdropper is supposed to move.

The remainder of this article is organized as follows. Sec. II describes the system model; the framework for the evaluation of the secrecy capacity over a surface is introduced, including all the parameters on which it depends, antenna orientation and pattern, nodes position and power, etc. In Sec. III, the new metric called secrecy pressure is defined. Sec. IV proposes the optimization problems, analytical solutions and graphs. In Sec. V some practical application scenarios are considered; antenna orientation as well as friendly jammer problems are solved in specific scenarios: from forbidden zone to mobility of the eavesdropper. In Sec. VI the closed-form of the secrecy outage probability of a surface is derived and discussed. Sec. VII concludes the paper.

II. System Model

Consider a 2D surface S described by Cartesian coordinates (x, y). Into this space there are the legitimate transmitter (node i) and receiver (node j), as well as a given number of interferers I_k with $k = 1, \cdots, N_I$ (Fig. 1). For better comprehension, let's assume that the space is a geographical urban area, the transmitter is a base station, the receiver is a mobile terminal and the interferers are other base stations or access points. We do not assume any specific position for the eavesdropper in the space. In fact, we want to derive how the secrecy is mapped all over the given environment.

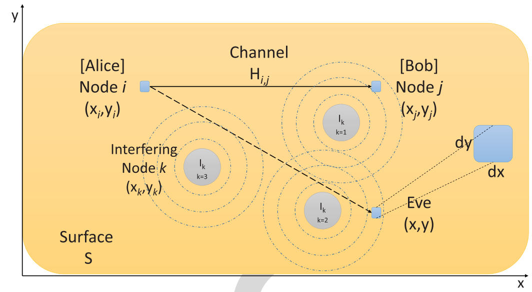


Fig. 1. General scenario. Two legitimate nodes (i and j) want to exchange a confidential message. They are immersed in an environment S together with interfering nodes I_k. The eavesdropper node can be located anywhere over the surface.

A. The Scenario

We assume to have a surface S where Alice and Bob are located and their position is known (Fig. 3). In the environment S there are also interfering nodes, whose positions are also known. Interfering nodes could be intentional jamming sources or simply other systems (base stations) radiating in the same frequency band of the legitimate transmission. To simulate this scenario, the position of Alice and Bob was chosen deterministically, while the position of the interfering nodes were randomly selected, by using a Point Poisson Process (PPP) distribution. The use of a PPP distribution for interfering nodes dispersion around a receiver is common in the literature, when dealing with security of wireless communications. Alice wants to transmit a confidential message M to Bob. The legitimate receiver (Bob) tries to recover the message from the observation vector Z_B. The eavesdropper (Eve) can be located anywhere in the surface S, and tries to recover the message M by analyzing the observation vector Z_E. The wireless channels from Alice to Bob and to Eve are supposed to be statistically independent.

B. Channel Model

Let us suppose to have two nodes on the surface S, a transmitting node i with position (x_i, y_i) and a receiving node j with position (x_j, y_j). The channel between node i and node j is modeled as

$$H_{i,j} = h_{i,j}(\tau, \psi) \cdot d_{i,j}^{-b} \tag{1}$$

where $d_{i,j}$ is the Euclidian distance between the nodes, b is the path loss exponent and $h_{i,j}(\tau, \psi)$ models the multipath fading effect, including angular dispersion

$$h_{i,j}(\tau, \psi) = \sum_{l=1}^{L} h_{i,j}^{(l)} \delta(\tau - \tau_l) \delta(\psi - \psi_j) \tag{2}$$

The parameter τ_l is the delay of arrival of the l-th path, while ψ_l is the angle of arrival of the l-th path, i.e., τ and ψ are modeling the time and angular dispersion of the multiple echoes arriving at the receiver, respectively. The variable $h_{i,j}^{(l)} = a_{i,j}^{(l)} e^{-\beta_{i,j}^{(l)}}$ denotes the channel coefficient, where $a_{i,j}^{(l)}$ is modelled as a stochastic variable with Rayleigh distribution

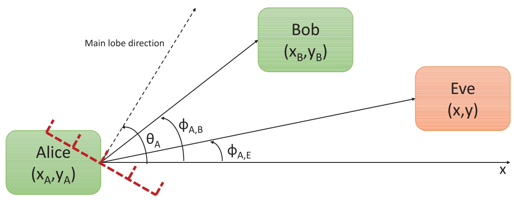


Fig. 2. Antenna pattern of the legitimate transmitter (Alice).

whose probability density function (PDF) is

$$f_{a_{i,j}^{(l)}}(a) = \frac{2a}{\sigma_a} e^{\frac{-a^2}{\sigma_a}}$$

with σ_a representing the standard deviation of the Rayleigh distribution, and $\beta_{i,j}^{(l)}$ is modeled as a stochastic random variable with uniform distribution in $(0, 2\pi)$. Each link that connect two nodes on the surface is supposed to have a fading coefficient which is independent to all others.

C. Received Power

Let us suppose that the node i is transmitting with power P_i. The power received by the node j is

$$P_j = P_i |H_{i,j}|^2 G_i(\theta_i, \phi_{i,j}) G_j(\theta_j, \phi_{j,i}) \tag{3}$$

where $G_i(\theta_i, \phi_{i,j})$ is the antenna pattern gain of the transmitter, $\phi_{i,j}$ is the angle between the x-axis and the segment connecting node i and j, and θ_i is the angle between the x-axis and the direction of maximum radiation (main lobe) of i-node's antenna. Fig. 2 shows the angles mentioned above, when node i is the legitimate transmitter, called Alice, and node j is the legitimate receiver, called Bob.

Defining $\tilde{P}_{i,j} = P_i G_i(\theta_i, \phi_{i,j}) G_j(\theta_j, \phi_{j,i})$ we can rewrite (3) as

$$P_j = \tilde{P}_{i,j} |H_{i,j}|^2 \tag{4}$$

Given the position of node i and j on the surface S, the angles $\phi_{i,j}$ and $\phi_{j,i}$ are fixed. Then, $\tilde{P}_{i,j} = \tilde{P}_{i,j}(\theta_i, \theta_j)$. If, in addition, the receiving node j has isotropic antenna $\theta_j = \text{Const}\ \forall j$, then $\tilde{P}_{i,j} = \tilde{P}_{i,j}(\theta_i)$.

According to [18] and [19], the time dispersion of the multipath at the receiver has an exponential distribution

$$f_\tau(\tau) = \frac{1}{\sigma_\tau} e^{-(\tau - \tau_0)/\sigma_\tau}$$

while the angle dispersion of the multipath at the receiver has a Laplacian distribution

$$f_\psi(\psi) = \frac{1}{\sqrt{2\sigma_\psi^2}} e^{-\sqrt{2}(\psi - \psi_0)/\sigma_\psi}$$

In order to average out the time and angular dispersion, the power P_j has to be integrated over all possible times and angles of arrival

$$\overline{P}_j = \tilde{P}_{i,j} d_{i,j}^{-2b} \int_\tau \int_\psi |h_{i,j}(\tau, \psi)|^2 f_\tau(\tau) f_\psi(\psi) d\tau d\psi \tag{5}$$

D. Aggregate Interference

Let us suppose that the N_I interfering nodes are distributed on the surface S following a point Poisson process (PPP) distribution with density λ. The sum of the interference power at the node j is

$$\begin{aligned} \mathbf{I}_j &= \sum_{k=1}^{N_I} P_k G_k(\theta_k, \phi_{k,j}) G_j(\theta_j, \phi_{j,k}) d_{k,j}^{-2b} |h_{k,j}|^2 \\ &= \sum_k \tilde{P}_{k,j} |H_{k,j}|^2 \end{aligned} \tag{6}$$

where P_k is the power emitted by the k-th interfering node, $d_{k,j}$ is the Euclidian distance between the k-th interfering node and node j and $h_{k,j}$ is the channel coefficient associated to the link (1). If the position of the N_I interfering nodes (x_k, y_k) with $k = 1, \cdots, N_I$ is fixed, then $\tilde{P}_{k,j} = \tilde{P}_{k,j}(\theta_k, \theta_j)$. If, in addition, the receiving node j has isotropic antenna $\theta_j = \text{Const}\ \forall j$, then $\tilde{P}_{k,j} = \tilde{P}_{k,j}(\theta_k)$. In this case, the aggregate interference $\mathbf{I}_j$ is a random variable with Stable distribution [16], [17]

$$\mathbf{I}_j \sim \mathcal{S}(\alpha, 1, \gamma_j) \tag{7}$$

where $\alpha = 1/b$ and

$$\gamma_j = \pi \lambda \Xi_\alpha^{-1} \mathbb{E} \left\{ \left(\sum_k \tilde{P}_{k,j} |h_{k,j}|^2 \right)^\alpha \right\}$$

with

$$\Xi_\alpha = \begin{cases} \dfrac{1-\alpha}{\Gamma(2-\alpha)\cos(\pi\alpha/2)} & \text{if } \alpha \neq 1 \\ \dfrac{2}{\pi} & \text{if } \alpha = 1 \end{cases} \tag{8}$$

where $\Gamma()$ denotes the Gamma distribution function and $\mathbb{E}\{\}$ the expectation operator.

The PDF of $\mathbf{I}_j$ is

$$\begin{aligned} f_{\mathbf{I}_j}(I) &= \frac{1}{2\pi} \int \varphi_I(\omega) e^{-j\omega I} d\omega \\ &= \frac{1}{\pi} \int_0^\infty e^{-\omega^\alpha \gamma_j} \cos\left[\tan\left(\frac{\pi\alpha}{2}\right) \omega^\alpha \gamma_j - \omega I\right] d\omega \end{aligned} \tag{9}$$

where

$$\varphi_I(\omega) = \exp\left\{-|\omega|^\alpha \left[1 - j\,\text{Sgn}(\omega) \tan\left(\frac{\pi\alpha}{2}\right)\right] \gamma_j\right\}$$

is the characteristic function of the random variable I.

It is important to highlight that depending on the position of the receiver j on the surface S, not all the N_I interferers could affect the receiver. The distance (path loss) $d_{k,j}^{-2b}$ could be close to zero, thus the node k does not contribute to the aggregate interference at the receiver j.

III. Secrecy Pressure and Secrecy Force

We want to define a new metric that allows to measure the intensity of secrecy over a given surface. Taking analogy from the atmospheric weather science, we define the concept of *Secrecy Pressure*.

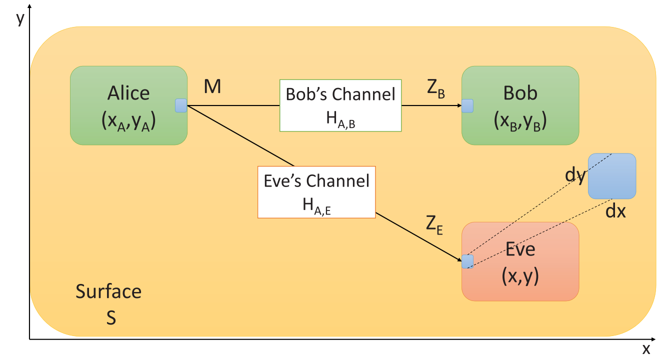


Fig. 3. Scheme of the transmission of the confidential message M from Alice to Bob.

Let us now associate the previous defined transmitting node i as Alice and the receiving node j as Bob. Alice is then located at point (x_A, y_A) and Bob at (x_B, y_B) on the surface S. The position of the eavesdropper Eve is not known, thus we suppose that its coordinates are generically (x, y).

Suppose that Alice wants to transmit a confidential message M to Bob. Bob tries to recover the information M from the vector Z_B received (Fig. 3). Given the model in Sec. II, the mutual information exchanged in the legitimate link (from Alice to Bob) is

$$\mathbb{I}_B = \mathbb{I}(M; Z_B) = \mathbb{H}(M) - \mathbb{H}(M|Z_B) \quad (10)$$

where $\mathbb{H}()$ denotes the entropy.

Analogously, the eavesdropper (Eve) tries to recover the message M from the received vector Z_E. Thus, the information stolen by Eve is

$$\mathbb{I}_E = \mathbb{I}(M; Z_E) = \mathbb{H}(M) - \mathbb{H}(M|Z_E) \quad (11)$$

The term $\mathbb{I}(M; Z_E)$ is called Leakage, and it denotes the amount of information on the message M that Eve is able to recover from the received vector Z_E.

As known, these two mutual information can be used to calculate the secrecy capacity [15]

$$C_{sec} = \max_{\mathfrak{p}_M} \{\mathbb{I}_B - \mathbb{I}_E\} \geq \max_{\mathfrak{p}_M} \mathbb{I}_B - \max_{\mathfrak{p}_M} \mathbb{I}_E = C_B - C_E \quad (12)$$

where C_B and C_E are the capacities of Bob's and Eve's channel, respectively, and $\mathfrak{p}_M$ is the marginal distribution of the codeword M. The secrecy capacity is at least as large as the difference between the legitimate channel capacity and the eavesdroppers channel capacity. The inequality can be strict as in the case of complex Gaussian wiretap channels [15], as well as typical wireless fading channels, which are here considered. It is important to note that both $\mathbb{I}_B$ and $\mathbb{I}_E$ depend on the channel state and position of Bob and Eve respect to Alice, respectively. This means that changing the position of Bob or Eve on the surface S, the mutual information changes.

The capacity of the link between the transmitter, called Alice, positioned in (x_A, y_A), and the position (x_B, y_B) of the legitimate receiver, called Bob, can be written as

$$C_B = \frac{1}{2} \log \left(1 + \frac{P_B}{N_0 + \mathbf{I}_B}\right) \quad (13)$$

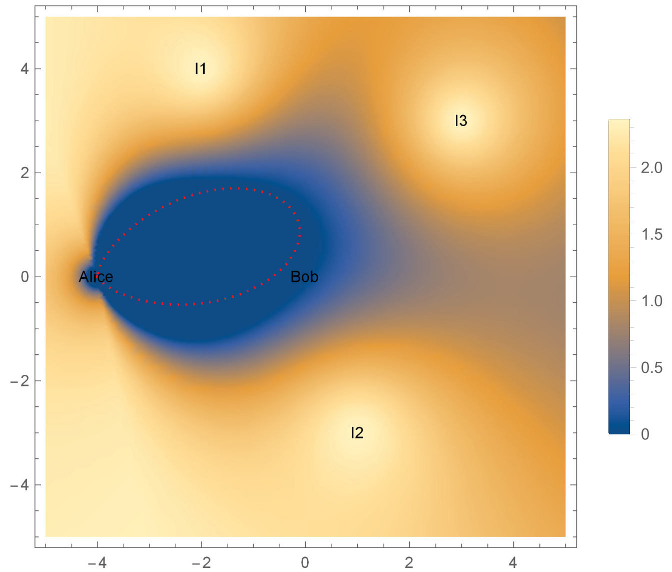


Fig. 4. Secrecy map of surface S with Alice's antenna orientation and pattern. Three interfering nodes (I_1, I_2, I_3) are present. The azimuth of Alice transmission antenna is 6 deg.

where N_0 denotes the Gaussian noise density at the receiver, P_B and $\mathbf{I}_B$ are defined in (4) and (6), respectively.

Since typically we cannot know if an eavesdropper, called Eve, is present in the surface S or where it is located, we derive the capacity of a generic point (x, y) of the surface, i.e.,

$$C_E(x, y) = \frac{1}{2} \log \left(1 + \frac{P_E}{N_0 + \mathbf{I}_E}\right) \quad (14)$$

where P_E and $\mathbf{I}_E$ are defined as in (4) and (6), respectively

$$P_E = P_A G_A(\theta_A, \phi_{A,E}) G_E(\theta_E, \phi_{E,A}) d_{A,E}^{-2b} |h_{A,E}|^2$$

$$\mathbf{I}_E = \sum_{k=1}^{N_I} P_k G_k(\theta_k, \phi_{k,E}) G_E(\theta_E, \phi_{E,k}) d_{k,E}^{-2b} |h_{k,E}|^2$$

Thus, supposing that Eve is located in a generic point (x, y) on the surface S, the secrecy capacity of the link between Alice and Bob is

$$C_{sec}(x, y) = \max\{0, C_B - C_E(x, y)\} = [C_B - C_E(x, y)]^+ \quad (15)$$

It is important to highlight that the capacities here are intended as conditioned to the state of the channels $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$, as well as the state of the aggregate interference $\mathbf{I}_B$ and $\mathbf{I}_E$.

What we are proposing here is to define a secrecy capacity for each elementary point (x, y) of the surface S. Using this representation, we can elaborate a map of the secrecy of the surface given the position of the known actors, i.e., legitimate users and interfering nodes. In other words, given the positions of Alice, Bob and interfering nodes I_k, for each point (x, y) of the surface, we calculate the secrecy capacity of the legitimate link as Eve was located in that point. The result is that we can draw a map showing the different levels of secrecy of the entire surface S (Fig. 4).

The *Secrecy Pressure* p_{sec} is defined as

$$p_{sec} = \frac{1}{A_S}\iint_S C_{sec}(x,y)dxdy = \frac{F_{sec}}{A_S} \tag{16}$$

where A_S denotes the area of the surface S and the term F_{sec} is denoting what we define as *Secrecy Force*. The secrecy force depends on the locations of the legitimate users and interfering nodes, but not on the eavesdroppers. The metric p_{sec} is a useful parameter that indicates how much is secure a surface S, given the position of legitimate nodes and interfering nodes. Using this metric, different surfaces and/or nodes configurations can be thus ordered

$$p_{sec}^{(1)} < p_{sec}^{(2)} < p_{sec}^{(3)} < \cdots$$

The index allows a ranking of a given spatial configuration of legitimate entities and interferes.

Detailing Eq. (16), we can find an interesting property of the secrecy pressure

$$p_{sec} = \frac{1}{A_S}\int_x\int_y \begin{cases} 0 & \text{if } C_B \le C_E(x,y) \\ C_B - C_E(x,y) & \text{if } C_B > C_E(x,y) \end{cases} dxdy \tag{17}$$

Since C_B does not depend on (x, y), if the surface goes to infinity, the secrecy pressure tends to a constant value

$$\lim_{S\to\infty} p_{sec} = \lim_{S\to\infty}\left(\frac{1}{A_S}\iint_S [C_B - C_E(x,y)]^+ dxdy\right) = C_B \tag{18}$$

This is because the path loss component $d_{A,E}^{-2b}(x,y)$ in (3) vanishes as the generic point (x, y) on the surface S goes to infinity. In practice, the contributions that decrease the secrecy pressure mainly comes from the points on the surface close to the legitimate link. In other words, supposing to have an infinite surface, the set of points where Eve could be located that influence the secrecy capacity is limited, due to the path-loss. A point (x, y) too far away from the legitimate nodes cannot affect the secrecy capacity, since the legitimate signal is received with a too low power to observe anything ($C_E(x, y) = 0$).

From Eq. (15) we can derive another useful representation, called *Secrecy Map*. The $C_{sec}(x, y)$ in (15) is indicating which is the secrecy capacity insisting over the elementary unit surface $dxdy$ located in a generic point (x, y) of the surface S (see Fig. 3). This representation can be used to draw the behaviour of the secrecy capacity over the surface S, showing zones where the secrecy is low or high, analogously to the weather forecast (Fig. 4). The map, in fact, is built by calculating the secrecy capacity of the legitimate link as the eavesdropper was located in each point of the surface. The blue zones in Fig. 4 indicate no secrecy, i.e., if the eavesdropper is set there, the secrecy rate of the legitimate link is zero. Summarizing, the secrecy map is derived by the following steps:

1) take a surface with cartesian coordinates;
2) locate the legitimate nodes (Alice and Bob) on the surface;
3) compute the secrecy capacity of the legitimate link assuming that Eve is located in a point (x,y) of the surface;
4) associate that secrecy capacity to the corresponding point of the surface;
5) repeat 3 and 4 for every point of the surface.

The secrecy capacity associated to a generic point of the surface could be zero, i.e., any time Eve has a greater channel capacity compared to Bob.

The secrecy map of the surface S changes with

- the positions of Alice, Bob and interfering nodes I_k ($k = 1, \cdots, N_I$);
- the pattern and the orientation $G_A(\theta_A)$ of the legitimate transmitter antenna;
- the power of the legitimate transmitter P_A;
- the power of the transmitters of the interfering nodes P_k;
- the state $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$ of the channels.

The effect of time and angle dispersion at the receivers can be averaged out by replacing $\overline{P}_j$ with $j = B$ in (13) and with $j = E$ in (14).

As listed in the above items, the secrecy capacity in (15) depends on the instant fading coefficients $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$. This means that the secrecy pressure (16) (and the secrecy map) depends instantly on these processes. In order to remove the dependance on the instantaneous realizations of the fading coefficients, two solutions can be run: 1) put the characteristic function of the fading coefficients into the secrecy capacity formula and average it out, or more easily, 2) assume that the channels are ergodic. The results shown in this paper are calculated by supposing ergodic channels. Ergodic-fading model characterizes a situation in which the duration of a coherence interval is on the order of the time required to send a single symbol. The processes $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$ are mutually independent and i.i.d.; fading coefficients change at every channel use and a symbol experiences many fading realizations.

The ergodic secrecy capacity is thus [15]

$$\widetilde{C}_{sec}(x,y) = \mathbb{E}_{|h_{A,B}|^2,|h_{A,E}|^2,|h_{k,B}|^2,|h_{k,E}|^2}\left\{[C_B - C_E(x,y)]^+\right\} \quad k = 1,\cdots,N_I \tag{19}$$

where the operator $\mathbb{E}\{\}$ stands for the expectation. The ergodic secrecy pressure is obtained by substituting the ergodic secrecy capacity in (19) into Eq. (16)

$$\widetilde{p}_{sec} = \frac{1}{A_S}\iint_S \widetilde{C}_{sec}(x,y)dxdy \tag{20}$$

Since $\widetilde{C}_{sec}(x, y)$ could be zero in some points of the surface, computing $\widetilde{p}_{sec}$ implies to make an integral of an irregular function.

It is important to point out that the power received by Eve depends on the position of Eve, since path-loss, fading, angle-of-departure, angle-of-arrival, as well as the power of the aggregate interference are position-dependent parameters. Therefore, in the expression of the capacity of both Bob and Eve, the parameters are position-dependent. Since we want a metric which is not dependent on the position of Eve (its position is not known with 100% probability, typically),

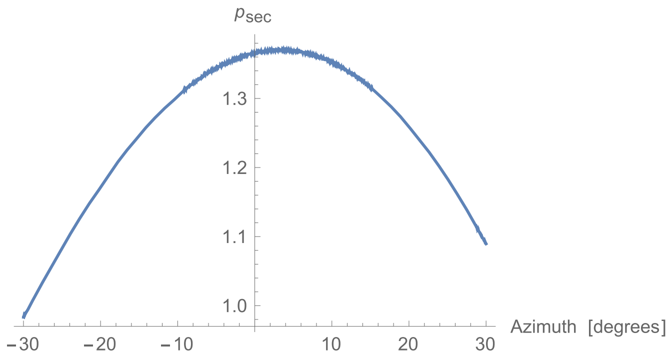


Fig. 5. Secrecy pressure when the optimization problem is solved respect to Alice's antenna orientation.

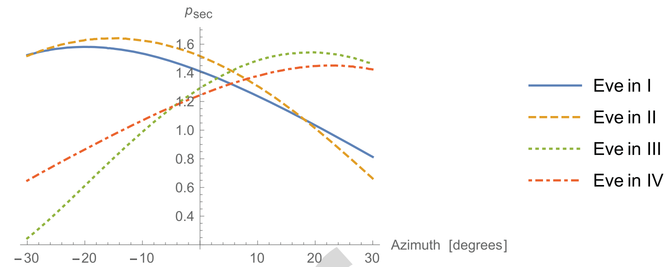


Fig. 6. Secrecy map for different positions of Eve (I, II, III and IV quadrant) when the optimization problem is solved respect to Alice's antenna orientation.

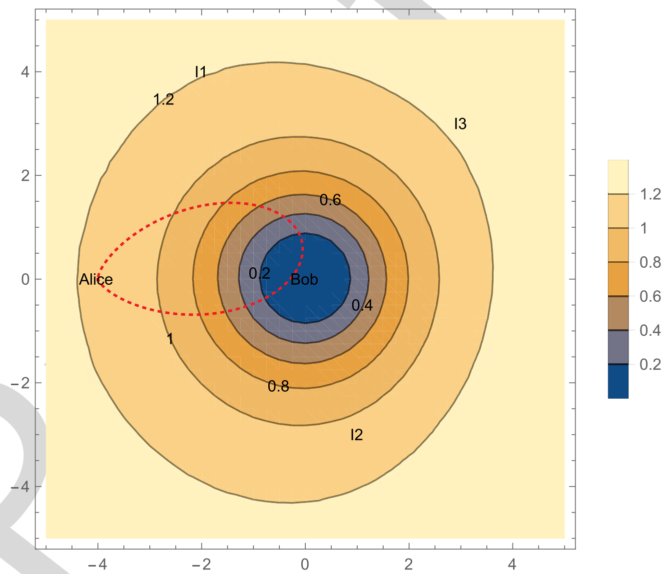


Fig. 7. Secrecy map over the surface S when the optimization problem is solved respect to the position of the additional interfering node (flasher).

we first locate Eve in each point (x,y) of the surface S, we calculate the secrecy capacity of each point (x,y) and then we integrate over the entire surface S. In this way, we take the mean over a space of the secrecy capacity, which eliminates the dependence of the secrecy capacity by specific position of Eve. The resulting (new) metric is a characteristic of the surface and not of the link, thus we called it secrecy pressure.

IV. Secrecy Optimization

The secrecy pressure can be used as a useful metric to determine which is the best configuration parameters to optimize the secrecy of a link. The proposed metric is suitable to find out different useful results, such as: a) which is the antenna orientation that assures highest secrecy towards the legitimate receiver; b) where is the best location where to put additional interfering node(s) in order to reach higher secrecy for the legitimate link; c) which is the best configuration of power emissions from the interfering nodes in order to have highest secrecy for the legitimate link.

A. Antenna Orientation

Let us suppose for simplicity that the interfering nodes I_k as well as Bob and Eve have isotropic antennas. Fixed the surface S, the positions of the legitimate nodes (Alice, Bob) and of the interfering nodes I_k ($k = 1, \cdots, N_I$), and given the pattern of the transmitting antenna $G_A(\theta_A)$, we can maximize the secrecy pressure respect to the antenna orientation

$$\arg \max_{\theta_A} \{p_{sec}\} \tag{21}$$

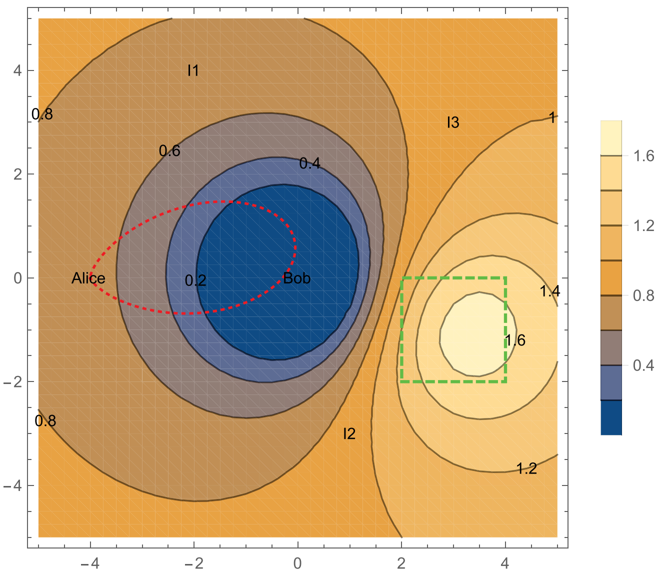
Fig. 5 shows the secrecy map over the surface S when Eve is supposed to be set somewhere in the surface S and the optimization problem is solved respect to Alice's antenna orientation. There exists an optimum azimuth orientation of Alice's antenna. Given the positions of the legitimate users and interfering nodes, the best, from the secrecy capacity point of view, for Alice is not to point the maximum of the antenna pattern towards the direction of Bob. An azimuth orientation of +6 deg optimizes the secrecy capacity, in this case. In general, with the proposed metric it is possible to derive easily which is the best antenna orientation for the transmission to a legitimate receiver in a given perimeter, of which we know only the positions of the interferers (e.g., other access points or base stations). Fig. 6 shows the secrecy map over the surface S for different positions of Eve (I, II, III and IV quadrant) when the optimization problem is solved respect to Alice's antenna orientation. As an example, suppose that the legitimate users do want to minimize the information leakage in a specific zone of the surface (e.g., the eavesdropper is suspected to be in the third quadrant), then the optimum antenna orientation for Alice is +16 deg (green curve in Fig. 6).

B. Interfering Node Positions

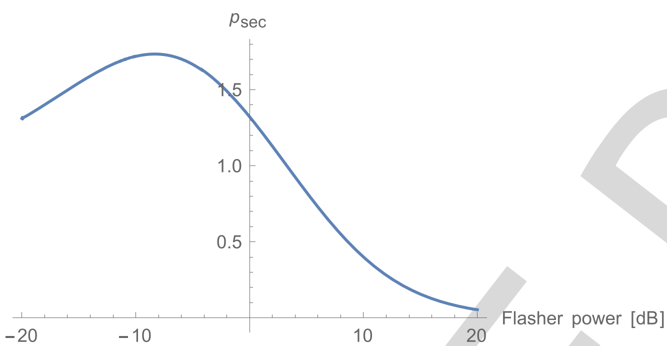
Fixed the surface S, the positions of the legitimate nodes (Alice, Bob) and given the pattern and orientation of the transmitting antenna $G_A(\theta_A)$, we can maximize the secrecy pressure over the position (x_k, y_k) of the $N_I + 1$-th interfering node, a friendly jammer called here *flasher*, in order to maximize the secrecy pressure of the legitimate link, given the positions (fixed) of the N_I interfering nodes

$$\arg \max_{(x_k, y_k),\ k=N_I+1} \{p_{sec}\} \tag{22}$$

Fig. 7 shows the secrecy map over the surface S when the optimization problem (22) is solved. As it can be seen, there are positions where the additional interference node (flasher)



(a) Secrecy map over the surface S when the optimization problem is solved respect to the position of the additional interfering node (flasher). Eve is supposed to be somewhere in the green dotted line.



(b) Secrecy pressure as a function of the power of the additional interfering node (flasher). The flasher is supposed to be placed in the center of the lighter zone depicted in Fig. 8(a).

Fig. 8. Optimization of both position and power of the additional interfering node (flasher).

can be put which optimize the secrecy pressure metric. Like forecast weather, the areas with same color bring the same secrecy capacity, if the additional interfering node (friendly jammer) is installed in that point of the surface. Another evident result is that the interfering node cannot be placed close to Bob (white hole in Fig. 7), since the this would decrease drastically the capacity of the legitimate link and thus the secrecy capacity. Fig. 8(a) shows the same secrecy map in the case that Eve is supposed to be somewhere in a limited perimeter (the green dotted line) inside the surface S. In this case the optimum area is modified compared to the previous scenario.

C. Power Allocation of the Interferers

Fixed the surface S, the positions of the legitimate nodes (Alice, Bob) and of the interfering nodes[2] I_k, and given the pattern and orientation of the transmitting antenna $G_A(\theta_A)$, we can maximize the secrecy pressure respect to the power emitted by the interfering nodes

$$\arg\max_{P_k} \{p_{sec}\} \quad k = 1, \cdots, N_I \tag{23}$$

To ease the illustration of this optimization, let us suppose to put an additional interfering node (the 4th) in the scenario and to optimize its transmit power. Figs. 8(a) shows the secrecy map over the surface S when the optimization problem is solved respect to the position of the additional interfering node (flasher) and its power. The eavesdropper is supposed to be located somewhere in a limited perimeter (the green dotted line in the figure) of the surface. The lighter zone of the secrecy map denotes the set of points (x,y) where the flasher can be located to yield the highest secrecy pressure. Fig. 8(b) shows the secrecy pressure as a function of the power of the flasher. The curve evidently shows an optimum point, which in that case is about -9 dB.

It is important to stress that using the proposed metric the optimum antenna orientation is not trivially in the direction of the legitimate receiver, as well as the optimum position and power of the intentional jammer (flasher) are not those that the common sense would suggest.

D. Joint Optimization

Joint optimization of all the parameters (antenna orientation, friendly jammer position and interfering power allocation) is also possible

$$\arg \max_{(\theta;(x_k,y_k);P_k)} \{p_{sec}\} \quad k = 1, \cdots, N_I \tag{24}$$

Graphical results of this optimization are not shown in this paper due to the lack of space.

E. Varying the Position of Bob

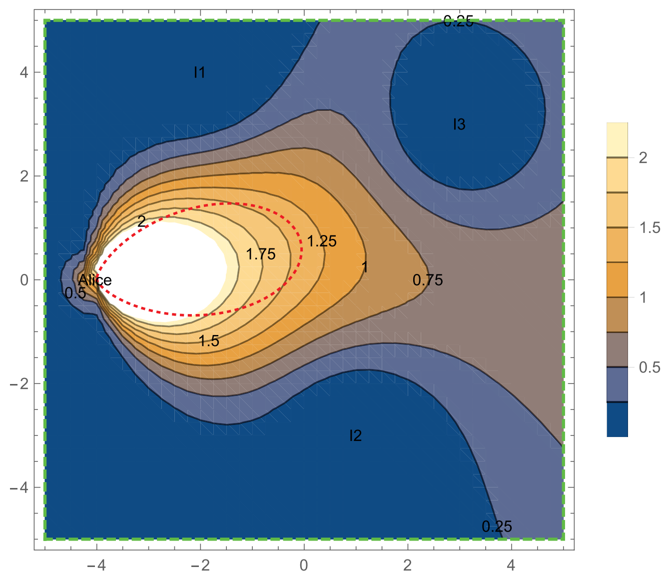
Although the most practical scenario is when Alice and Bob are fixed and Eve can be everywhere in a limited space, as previously described, one could also be interested in using the proposed metric to draw the map of the secrecy pressure when Bob's position can vary over the surface S. In this case, the steps to draw the map are the following

- locate the legitimate receiver (Bob) in a point (x, y) of the surface S;
- calculate the secrecy pressure metric (20) for Bob located in that point;
- assign to the point (x, y) the value of the secrecy pressure;
- repeat these points until all the surface S is evaluated.

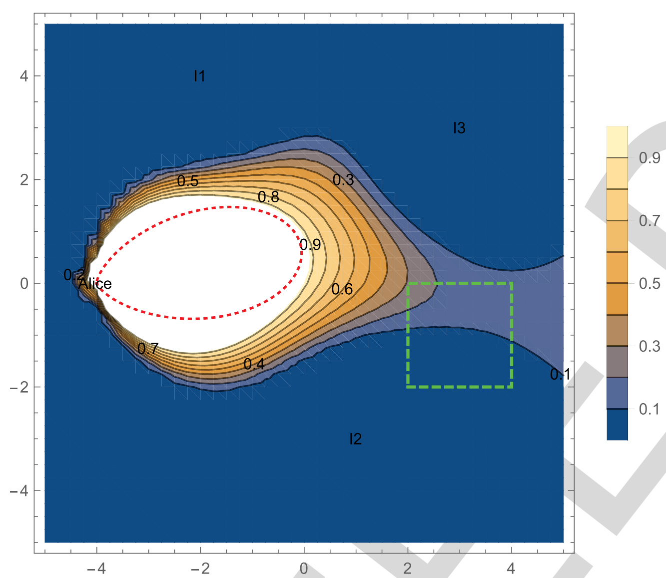
Fig 9(a) shows the map of the secrecy pressure when Bob's position varies over the surface and Eve's position varies over the entire surface as well. As expected the secrecy pressure is higher when Bob is inside the main lobe of Alice, while the secrecy pressure decreases drastically when Bob is closer to an interferer.

Fig 9(b) shows the map of the secrecy pressure when Bob's position vary over the surface and Eve's position varies only in a limited perimeter (the green dashed line). Compared to Fig 9(a), if Eve is confined into a limited space in

[2]The position of the interfering nodes has been randomly selected by using a PPP distribution.



(a) Map of the secrecy pressure as a function of Bob's position. Eve can be everywhere over the surface.



(b) Map of the secrecy pressure as a function of Bob's position. Eve is supposed to be somewhere in the green dotted line.

Fig. 9. Map of the secrecy pressure. The secrecy pressure is calculated as Bob was in each point (x, y) of the surface S.

the surface S, the zone of maximum secrecy pressure is larger and located around the main lobe of Alice. Please note that the secrecy pressure behind Alice, e.g. the point $(-4, -2)$, is low since there is almost no power from Alice in that direction.

V. General Definition of Secrecy Pressure and Practical Applications

As stated in the previous sections, the new metric is defined starting from the definition of the well-known secrecy capacity (C_{sec}). To eliminate the dependence on the position of the eavesdropper of the secrecy capacity, we have averaged out the secrecy capacity by integrating the C_{sec} over the 2D-space of the specific surface S. The resulting metric is called secrecy pressure and it is the analytical expression of the average over a space (instead of time). The integral of the C_{sec} function is not easy to derive, since C_{sec} shows sparsely zeros over the 2D surface, each time that the capacity of Eve is greater of the capacity of Bob. A closed-form expression of the secrecy pressure is not easy to obtain, even for simple geometry shape like circle or square with generic boundaries. For this reason, we have derived the closed-form expression of the secrecy outage of a surface (see Sec. VI). Although a closed-form expression of the secrecy pressure for a known shape is not shown in the paper, this does not mean that the metric makes no sense. The metric is defined as the spatial average of the secrecy capacity calculated for every point of the surface S. The average of the secrecy capacity over time is called ergodic secrecy capacity in the literature, but no previous paper, in our knowledge, presented the spatial average.

This metric shows the secrecy as a characteristic of a surface and not of a single link. This is useful in many practical scenarios, like military tactical scenarios. Typically, military command has a specific perimeter of operation, where the presence of the enemy is not perfectly known, based on the information that the intelligence service or technologies (satellite, etc.) can collect. Most probably, the military command can delimit the presence of the enemy in some zones of the operational scenario, associating the presence of the enemy with a certain probability. By calculating the secrecy pressure, the military command can: 1) quantify how much secure is one perimeter from the point of view of the wireless transmissions; 2) decide the optimum angle for the transmitting antenna array; 3) decide which is the optimum position to place a jammer to enhance the security of the transmission; 4) decide the optimum power of the jammer, in order not to degrade the reception of the legitimate receiver while jamming the potential eavesdropper; 5) operate a multi-parameter optimization; 6) if the position of the eavesdropper is only partially known, the military command can draw zones in the operational perimeter giving to each of them a statistical probability of Eve presence, and then compute the secrecy of the perimeter; 7) if a mobility model of Eve is known or partially (statistically) known, again all the above mentioned parameters (antenna orientation, friendly jammer position, etc.) can be optimized. Other optimizations can be further imagined.

As discussed above, in many practical situations we do not know if an eavesdropper is present and where it is located exactly. Thus, we define a probability of presence of Eve to be associated to a generic point (x, y) on the surface S

$$\Upsilon_{X,Y}(x, y) = Prob\{x \le X \le x + dx,\ \ y \le Y \le y + dy\}$$
$$= \int_{x}^{x+dx} \int_{y}^{y+dy} \upsilon_{X,Y}(x, y) dx dy \tag{25}$$

where $\upsilon_{X,Y}(x, y)$ is the probability density function (PDF) of the presence of Eve in (x, y). From now on we call this PDF $\upsilon_E(x, y)$.

The secrecy pressure is thus re-defined as follows

$$p_{sec} = \iint_S \upsilon_E(x, y) C_{sec}(x, y) dx dy \tag{26}$$

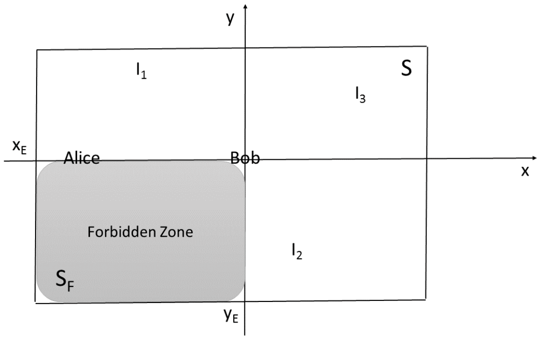


Fig. 10. Forbidden zone inside the surface S.

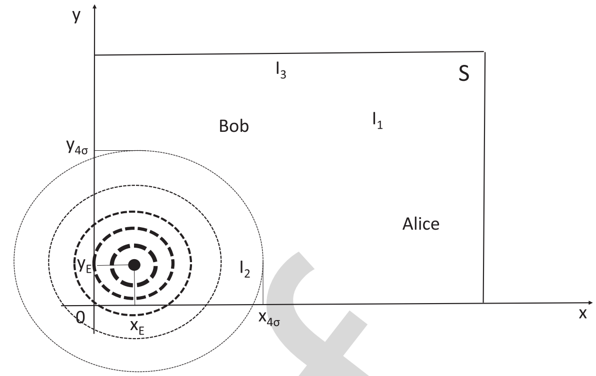


Fig. 11. Gaussian distribution of Eve's presence inside the surface S.

where $C_{sec}(x, y) = [C_B - C_E(x, y)]^+$ and $\iint \upsilon_E(x, y) dxdy = 1$. Eq. (26) represents the more general expression of the secrecy pressure in (16). For example, if a uniform distribution of Eve's presence is supposed for the entire surface S, the PDF would be $\upsilon_E(x, y) = 1/A_S$ and thus $\iint_S 1/A_S dxdy = 1$.

In the following sections three practical scenarios are proposed to show the benefits of the new proposed metric. In particular, the secrecy pressure is computed when

- an eavesdropper is known to be in a sub-region of the surface S (leakage zone),
- the eavesdropper position is known with a probability spatial function (Gaussian approximation), and
- when the eavesdropper has not a fixed position (mobility scenario).

In all these cases, some simplifications are assumed

- the average fading of the channels is supposed to be 1, i.e., $\sum_l |h_{i,j}^{(l)}|^2 = 1$;
- the antenna pattern of Bob, Eve and of the interfering nodes is supposed to be isotropic. Only Alice has a directive antenna and can modify the antenna orientation;
- the position of Alice and Bob on the surface S is supposed to be fixed and known: $(-4, 0)$ and $(0, 0)$, respectively;
- the position of the interfering nodes (I_1,I_2,I_3) is supposed to be fixed and known: $(-2, 4)$, $(1, -3)$ and $(3, 3)$, respectively.

A. Leakage Zone

In many real situations, e.g., in military scenarios, the transmitter does not want to leak information in fixed zone, in a region where it knows that an eavesdropper is surely present. We name here the leakage zone as *forbidden zone*, since the legitimate transmitter surely does not want to leak any information in that zone. Fig. 10 shows the surface S with the forbidden zone S_F inside. In this example the forbidden zone is the third quadrant.

To each point of the surface S_F we associate a probability of Eve's presence such that $\iint_{S_F} \upsilon_E(S)dxdy = 1$, while in the rest of the surface S we set $\iint_{\neg S_F} \upsilon_E(S)dxdy = 0$, where $\neg S_F$ denotes the complementary surface $S_F \cup \neg S_F = S$.

Assume, as an example, to have an equal distribution of the probability of Eve's presence in the surface S_F. Than,

$$\upsilon_E(x, y) = \begin{cases} \frac{1}{x_E y_E}, & \text{if } x \in [0, x_E] \text{ and } y \in [0, y_E] \\ 0, & \text{otherwise} \end{cases} \tag{27}$$

In this case the secrecy pressure of the surface (26) is

$$p_{sec} = \int_0^{x_E} \int_0^{y_E} \upsilon_E(x, y)C_{sec}(x, y)dxdy \tag{28}$$

The secrecy map of the surface can be drawn by using the following result

$$\upsilon_E(x, y)C_{sec}(x, y) = \begin{cases} 0 & \text{if } C_{sec}(x, y) = 0 \\ C_B - \frac{1}{x_E y_E} \int_0^{x_E} \int_0^{y_E} C_E(x, y)dxdy & \text{otherwise} \end{cases} \tag{29}$$

The optimization of the secrecy pressure respect to the azimuth of the transmitting antenna of the legitimate node (Alice) for a forbidden zone is shown in Fig. 5.

B. Gaussian Probability of Eavesdropper Presence

In other situations, it is not known exactly if eavesdroppers are present or not. Only suspicious. In this case, located a point on the map, a probability of presence of Eve with certain distribution can be associated. We suppose here that a Gaussian spatial distribution of Eve's presence is associated to a zone of the surface S. To each point of the surface S we associate a probability of Eve's presence υ_E which is a random variable with Gaussian distribution centered in (x_E, y_E) (Fig. 11). The circle lines denotes the intensity of the probability. For example, if the Gaussian random variable denoting the presence of Eve on the surface has mean 0.8 and variance 1, we associate a probability of Eve's presence equal to 0.8 to the point (x_E, y_E).

In this case the secrecy pressure of the surface (26) is

$$p_{sec} = \iint_S \upsilon_E(x, y)C_{sec}(x, y)dxdy \tag{30}$$

With $\upsilon_E(x, y) = \frac{1}{\sqrt{2\sigma_E^2}} e^{\frac{(x-x_E)^2+(y-y_E)^2}{2\sigma_E}}$, where σ_E indicates the standard deviation of the Gaussian distribution.

The secrecy map of the surface can be drawn by using the following result

$$\upsilon_E(x,y)C_{sec}(x,y)dxdy = \begin{cases} 0 & \text{if } C_{sec}(x,y) \le 0 \\ C_B - \iint_S \upsilon_E(x,y)C_E(x,y)dxdy & \text{otherwise} \end{cases} \tag{31}$$

This scenario is a particular case of the mobility scenario described in the next section, the results can be appreciated in Fig. 13(b).

C. Mobility Model for the Eavesdropper

If we know the position of Eve at time t_n, we can associate to the eavesdropper a statistical mobility model and derive the secrecy pressure over a surface of interest. The mobility model for Eve depends on its movement capability in the specific environment. In the absence of prior information on the real movement of the eavesdropper (i.e., Eve is free to move in all directions with different speeds), the Gaussian mobility model represents a fairly general model with a tractable number of parameters. In the presence of some prior information on the eavesdroppers movement (e.g., direction or speed is set by the environment), a mobility model more tight to the real mobility would provide better performance.

Optimization of the secrecy pressure is shown respect to the azimuth of the legitimate transmitting antenna as well as respect to the position of the flasher.

We consider here Gaussian mobility model with conditional PDF of current position conditioned on the previous position. For easier notation, let us define the position (x, y) at time t_n of a point on the surface S as a vector $\mathbf{p}_n$. Thus, the conditional PDF of current position is

$$\upsilon_m(\mathbf{p}_n|\mathbf{p}_{n-1}) = \frac{1}{2\pi|\Sigma_m|^{\frac{1}{2}}} e^{-\frac{1}{2}\left[(\mathbf{p}_n-\boldsymbol{\mu}_n)^T\Sigma_m^{-1}(\mathbf{p}_n-\boldsymbol{\mu}_n)\right]} \tag{32}$$

where $\boldsymbol{\mu}_n$ varies with the mobility model as described in the following, and the covariance matrix Σ_m accounts for the uncertainty in the movements in a 2-D plane; thus, it is expressed by

$$\Sigma_m = \begin{bmatrix} \sigma_{m,x} & \rho\sigma_{m,x}\sigma_{m,y} \\ \rho\sigma_{m,x}\sigma_{m,y} & \sigma_{m,y} \end{bmatrix} \tag{33}$$

where $\sigma_{m,x}$ and $\sigma_{m,y}$ is the standard deviation along the x and y axes, respectively. The parameter ρ takes into account the possible inter-dependence of the two coordinates. Independent coordinates have $\rho = 0$.

The mean $\boldsymbol{\mu}_n$ depends on the position $\mathbf{p}_{n-1}$ and the speed $\mathbf{v}_{n-1}$ according to

$$\boldsymbol{\mu}_n = \mathbf{p}_{n-1} + \mathbf{v}_{n-1}(t_n - t_{n-1}) \tag{34}$$

where $\mathbf{v}_{n-1}$ is the vector of the speed along x and y axes at time t_{n-1}.

Fig. 12 shows the secrecy map over the surface S as a function of the position of the flasher (22) and with mobility model for the eavesdropper (32). Eve is suspected to move vertically from its previous position, with a mobility model given by (32). The interfering nodes I_1, I_2 and I_3 are fixed.

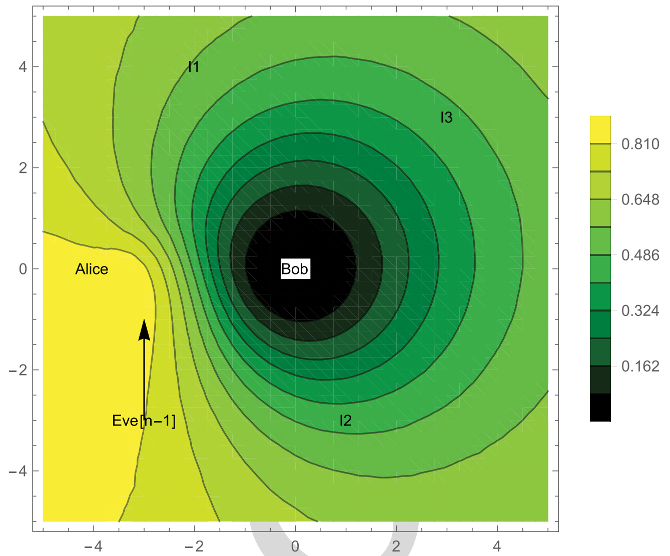


Fig. 12. Secrecy map of the position of the flasher with mobility model for the eavesdropper.

Solving (22) gives the optimum point where to locate the additional flasher I_4. Best is to put the flasher close to the point where the eavesdropper is supposed to arrive. This is somehow trivial.

In order to complicate the scenario we supposed that Eve is moving from $(3, -3)$ to $(3, 3)$ with a mobility model given by (32) (see Fig. 13(a)) in six time steps. Alice antenna azimuth orientation can vary from -30 to $+30$ deg. The resulting map of the secrecy pressure is shown in Fig. 13(b). The map shows which is the optimum transmit antenna orientation (azimuth) at each time step. As an example, at time step 6, Eve is stochastically supposed to be in $(3, 3)$ and thus an orientation between -18 to $+8$ deg optimizes the secrecy capacity for the Eve's mobility scenario. In this case the secrecy rate achievable is more than 3.20 bps. On the contrary, at time step 3 the maximum secrecy rate achievable is 1.28 bps with an antenna orientation range of $(-26, -20)$ deg.

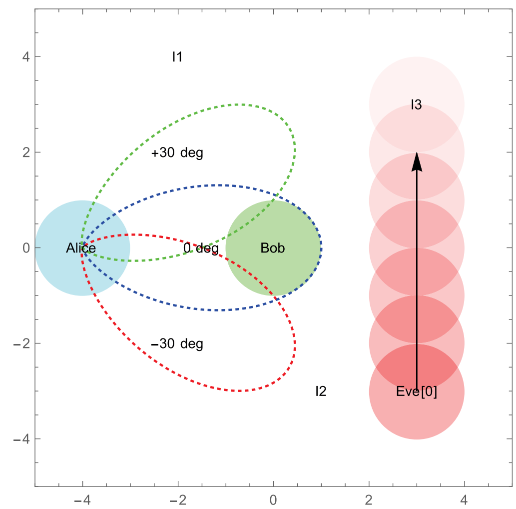
VI. Secrecy Outage Probability of a Surface (SOPS)

A closed-form of the secrecy pressure is not easy to be derived. Another interesting metric could be the outage probability of the secrecy capacity over a surface. A secure outage occurs when the instantaneous secrecy capacity $C_{sec}(x, y)$ is less than target secrecy rate $\overline{R}_{sec}$. Thus, the secure outage probability is defined as

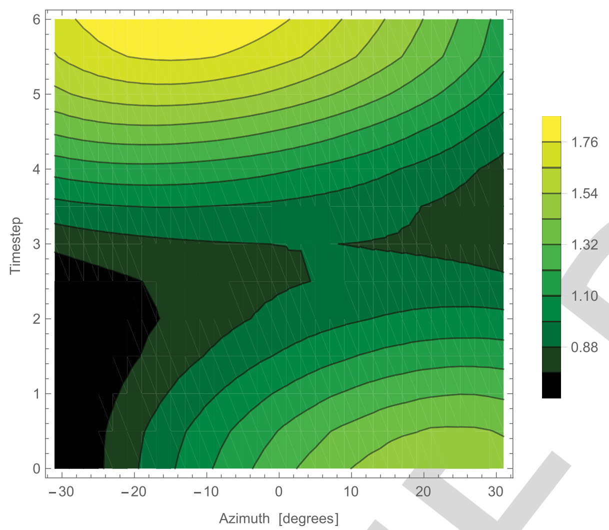
$$P_{out}(\overline{R}_{sec})(x,y) = \text{Prob}\{C_{sec}(x,y) < \overline{R}_{sec}\} \tag{35}$$

Note that the outage probability depends on the location (x, y) of the eavesdropper over the surface. Given the result above, we define the secrecy outage probability of a surface S (SOPS) as

$$\begin{aligned} A_{out}(\overline{R}_{sec}) &= \iint_S P_{out}(\overline{R}_{sec})(x,y)\upsilon_E(x,y)dxdy \\ &= \iint_S \text{Prob}\{C_{sec}(x,y) < \overline{R}_{sec}\upsilon_E(x,y)dxdy \end{aligned} \tag{36}$$



(a) Eve's mobility scenario.



(b) Secrecy map of the Alice's antenna orientation with mobility model for the eavesdropper.

Fig. 13. Eve's mobility: scenario description and secrecy map over azimuth of Alice's antenna.

The secrecy outage probability of a surface depends on the probability $\upsilon_E(x, y)$ that Eve is located in the point a generic point (x, y) of the surface. An interesting behaviour to study is the existence of the secrecy capacity over a surface, i.e., when $\overline{R}_{sec}$ is set to zero. In this case the SOPS becomes

$$A_{out}(\overline{R}_{sec} = 0) = \iint_S \text{Prob}\{C_{sec}(x, y) = 0\}\upsilon_E(x, y)dxdy \tag{37}$$

The term $\upsilon_E(x, y)$ is the distribution of the presence of Eve over the surface, which could be uniform or Gaussian or any other distribution, based on what it is known about the eavesdroppers. The term $\text{Prob}\{C_{sec}(x, y) = 0\}$ can be derived as

$$\text{Prob}\{C_{sec}(x, y) = 0\} = \text{Prob}\{SNR_E(x, y) \geq SNR_B\} \tag{38}$$

where

$$SNR_B = \frac{P_B}{N_0 + \mathbf{I}_B} \tag{39}$$

$$SNR_E(x, y) = \frac{P_E}{N_0 + \mathbf{I}_E} \tag{40}$$

with P_B, P_E defined as in (3) and $\mathbf{I}_B$, $\mathbf{I}_E$ as in (6). Eq. (38) is hard to be calculated analytically, since the term at numerator P_B is Rayleigh distributed, while the term at the denominator $\mathbf{I}_B$ is Stable distributed. A closed form can be reached if we assume that the Gaussian approximation is valid for the aggregate interference, i.e., $\mathbf{I}_B \sim \mathcal{N}(0, N_B)$ and $\mathbf{I}_E \sim \mathcal{N}(0, N_E)$. In this case Eq. (41) becomes

$$SNR_B = \frac{P_B}{N_0 + N_B} \tag{41}$$

$$SNR_E(x, y) = \frac{P_E}{N_0 + N_E} \tag{42}$$

and Eq. (38) can be written as [20]

$$\begin{aligned}\text{Prob}\{C_{sec}(x, y) = 0\} &= \text{Prob}\{SNR_E(x, y) \geq SNR_B\} \\ &= \frac{\overline{SNR}_E(x, y)}{\overline{SNR}_B + \overline{SNR}_E(x, y)}\end{aligned} \tag{43}$$

where

$$\overline{SNR}_i = \frac{\widetilde{P}_i d_{A,i}^{-b}\mathbb{E}\{|h_{A,i}|^2\}}{N_0 + N_i}$$

with $i = \{B, E\}$ and $\mathbb{E}\{\}$ is the expectation operator.

Thus, the SOPS in this case is

$$A_{out}(\overline{R}_{sec} = 0) = \int_x\int_y \frac{\overline{SNR}_E(x, y)}{\overline{SNR}_B + \overline{SNR}_E(x, y)}\upsilon_E(x, y)dxdy \tag{44}$$

In the case of a target secrecy rate greater than zero $\overline{R}_{sec} > 0$, Eq. (44) is

$$\begin{aligned}&A_{out}(\overline{R}_{sec}) \\ &= \iint_S \text{Prob}\{C_{sec}(x, y) < \overline{R}_{sec}\}\upsilon_E(x, y)dxdy \\ &= \int_x\int_y \left(1 - \frac{\overline{SNR}_B \cdot \exp\left\{-\frac{2^{\overline{R}_{sec}-1}}{\overline{SNR}_B}\right\}}{\overline{SNR}_B + 2^{\overline{R}_{sec}}\overline{SNR}_E(x, y)}\right)\upsilon_E(x, y)dxdy\end{aligned} \tag{45}$$

The results of the SOPS are shown in Fig. 14. The curves are derived by supposing a Gaussian distribution of the presence of Eve on the surface, i.e.,

$$\upsilon_E(x, y) = \frac{1}{\sqrt{2\sigma_E^2}}e^{\frac{(x-x_E)^2+(y-y_E)^2}{2\sigma_E}}$$

The other parameters are set as follows: $\mathbb{E}\{|h_{A,i}|^2\} = 1$ with $i = \{B, E\}$, σ_E ranges from 0.2 to 5.

Fig. 14 shows the SOPS ($A_{out}(\overline{R}_{sec} = 0)$) as a function of the standard deviation σ_E of the distribution of Eve's presence on the surface S. Eve is located in three different positions: at Alice's, at Bob's and at the first interferer's I_1. The positions of Alice, Bob and the interferers I_1, I_2 and I_3 are shown in Fig. 4.

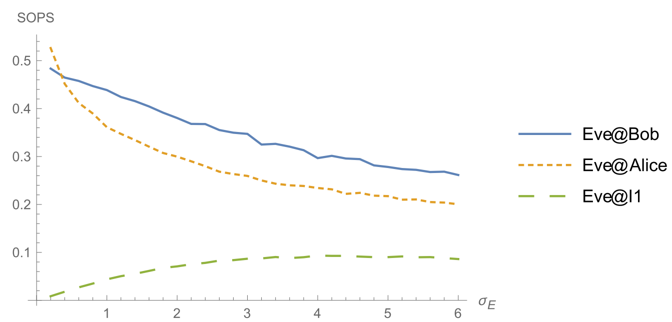


Fig. 14. Secrecy outage of the surface S as a function of the standard deviation σ_E of the distribution of Eve's presence over S. Eve's distribution is Gaussian and centered in three different positions: at Alice's, at Bob's and at the first interferer's I_1.

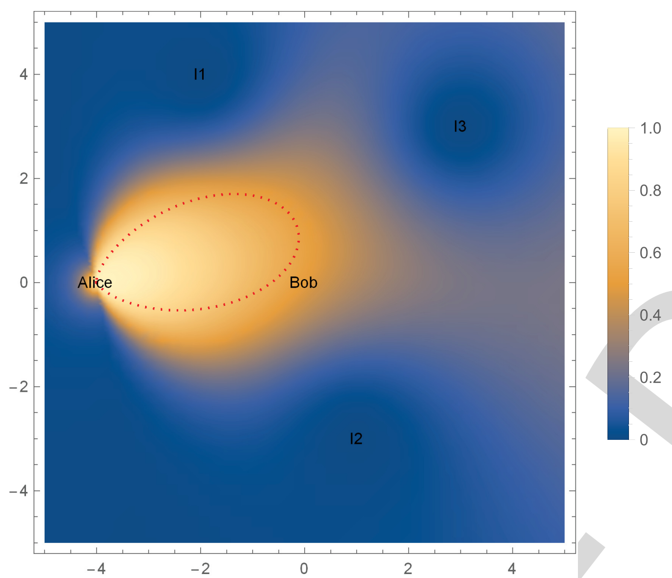


Fig. 15. Secrecy pressure outage map of the surface S.

The orange dotted line in Fig. 14 reports the results when Eve's distribution is centered on the same position of Alice. The curve of the SOPS confirms that a higher dispersion of the probability of Eve's presence yields a lower surface secrecy outage. This is logic, since a higher variance of the Gaussian distribution means higher probability that Eve is located far away from Alice. The green dashed line in Fig. 14 reports the results when Eve's distribution is centered on the same position of the first interferer I_1. The curve of the SOPS, in this case, are completely different from the previous one, as expected. The SOPS increases with the variance σ_E, since a higher dispersion of the position of Eve means a higher probability that Eve is located far away from the interference source, which jams Eve's receiver.

The blue solid line in Fig. 14 reports the results when Eve's distribution is centered on Bob's position. The SOPS increases with the variance σ_E, since a higher dispersion of the position of Eve means a higher probability that Eve is located closer to the source of the information (Alice), i.e., Eve's could have a better signal to noise ratio compared to Bob.

The secrecy pressure outage map of the entire surface is shown in Fig. 15.

VII. Conclusions

This paper proposes and studies a new metric for measuring the secrecy potentials of a surface. This metric is defined secrecy pressure. Using the metric different environments or surfaces can be ordered as a function of the secrecy rate that can be assured. The metric can be used also for solving optimization problems, e.g., finding which is the best transmit antenna orientation to maximize the secrecy capacity of the surface, or finding which is the best position of an additional interfering node (friendly jammer). Different practical scenarios are investigated, including mobility option for the eavesdropper. Another metric, the secrecy outage probability of a surface (SOPS), is derived. In this case the presence of Eve is supposed to be uncertain, and modelled as a Gaussian distribution over the surface. The results of the SOPS are shown as a function of the dispersion of Eve's position. The Gaussian distribution is centered in three specific points: at Alice's, at Bob's and at the first interferer's.

In addition the first part of the paper includes a general framework to evaluate the secrecy capacity over a surface. The framework includes all the parameters affecting the secrecy capacity, from nodes spatial distribution, to antenna orientation and pattern, and propagation medium statistics.

This paper offers a new perspective on the role of secrecy over a surface, considering nodes spatial distribution, wireless propagation medium, and aggregate network interference.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, Aug. 1975, p. 13551387.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Technol. Biomed.*, vol. 24, no. 7, pp. 451–456, Jul. 1978.

[3] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun.*, vol. 6, no. 3, pp. 311–335, Mar. 1998.

[4] Y. Zou, Y.-D. Yao, and B. Zheng, "Opportunistic distributed space-time coding for decode-and-forward cooperation systems," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1766–1781, Apr. 2012.

[5] S. Lakshmanan, C. L. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas, distributed computing systems," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Beijing, China, Jun. 2008, pp. 19–27.

[6] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

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

[8] M. P. Daly, E. Daly, and J. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[9] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 8, pp. 1478–1493, Aug. 2016.

[10] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. 13th Can. Workshop Inf. Theory (CWIT)*, Toronto, ON, Canada, Jun. 2013, pp. 214–218.

[11] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[12] J. M. Carey and D. Grunwald, "Enhancing WLAN security with smart antennas: A physical layer response for information assurance," in *Proc. Veh. Technol. Conf. (VTC Fall)*, Los Angeles, CA, USA, Sep. 2004, pp. 318–320.

[13] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 56–69, Feb. 2015.

[14] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment—Part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.

[15] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[16] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009.

[17] A. Rabbachin, A. Conti, and M. Z. Win, "The role of aggregate interference on intrinsic network secrecy," in *Proc. Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 3548–3553.

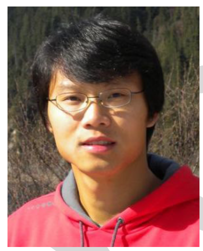
[18] K. I. Pedersen, P. E. Mogensen, and B. H. Fleury, "A stochastic model of the temporal and azimuthal dispersion seen at the base station in outdoor propagation environments," *IEEE Trans. Veh. Technol.*, vol. 49, no. 2, pp. 437–447, Mar. 2000.

[19] H. Asplund, A. A. Glazunov, A. F. Molisch, K. I. Pedersen, and M. Steinbauer, "The COST 259 directional channel model—Part II: Macrocells," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3434–3450, Dec. 2006.

[20] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory'(ISIT)*, Jul. 2006, pp. 356–360.

Lorenzo Mucchi (M'98–SM'12) received the Dr.Eng. (Laurea) degree in telecommunications engineering from the University of Florence, Italy, in 1998, and the Ph.D. degree in telecommunications and information society in 2001. Since 2001, he has been a Research Scientist with the Department of Information Engineering, University of Florence. In 2000, he spent a 12 month period of research at the Center for Wireless Communications, University of Oulu, Finland. He has been a Professor of information technologies with the University of Florence, since 2008. His main research areas include theoretical modeling, algorithm design, and real measurements, mainly focusing on physical-layer security, visible light communications, ultra wideband techniques, localization, adaptive diversity techniques, and interference management. He has authored or co-authored eight book chapters, 32 papers in international journals, and over 80 papers in international conference proceedings during his research activity. He was a member of the IEEE Communications and Information Security Technical Committee in 2009. Since 2016, he has been an Associate Editor of the IEEE COMMUNICATION LETTERS. In 2004, he was the Lead Organizer and the General Chair of the IEEE International Symposium on Medical ICT. He has been the Guest Editor and the Editor-in-chief of the Elsevier Academic Press Library. He was a member of the European Telecommunications Standard Institute Smart Body Area Network (SmartBAN) Group in 2013 and the Team Leader of the special task force 511 SmartBAN Performance and Coexistence Verification in 2016.

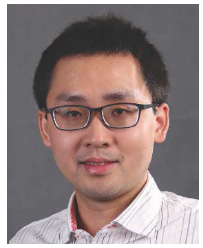
Luca Ronga (S'89–M'94–SM'04) received the M.S. degree in electronic engineering and the Ph.D. degree in telecommunications from the University of Florence, Italy, in 1994 and 1998, respectively. In 1997, he joined as a Visiting Scientist the International Computer Science Institute of Berkeley, CA. In 1999, he joined Italian National Consortium for Telecommunications, where he is currently heads the research area. He has authored over 90 papers in international journals and conference proceedings. His research interests span satellite communications to cognitive radio, software-defined radio, radio resource management, and wireless security. He has been an Editor of the *EURASIP Newsletter* for four years, a member of the ETSI SatEC Working Group, and a member of NATO Task Force on Cognitive Radio. He has been a principal investigator in several research projects.



Xiangyun Zhou (M'11) received the Ph.D. degree from The Australian National University (ANU) in 2010. He is currently a Senior Lecturer with ANU. His research interests are in the fields of communication theory and wireless networks. He was a recipient of the Best Paper Award at at ICC in 2011 and the IEEE ComSoc Asia-Pacific Outstanding Paper Award in 2016. He served as a Guest Editor of the *IEEE Communications Magazine* feature topic on wireless physical layer security in 2015. He has also served as the symposium, track, and workshop co-chair for major IEEE conferences. He was the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He currently serves on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE COMMUNICATIONS LETTERS.

Kaibin Huang (M'08–SM'13) received the B.Eng. degree (Hons.) and the M.Eng. degree from the National University of Singapore, and the Ph.D. degree from The University of Texas at Austin (UT Austin), all in electrical engineering. Since 2014, he has been an Assistant Professor with the Department of Electrical and Electronic Engineering (EEE), The University of Hong Kong. He was a Faculty Member with the Department of Applied Mathematics (AMA), The Hong Kong Polytechnic University (PolyU) and the Department of EEE, Yonsei University, South Korea, where he is currently an Adjunct Professor. He is also a University Visiting Scholar with Kansai University, Japan. His research interests focus on the analysis and design of wireless networks using stochastic geometry, and multi-antenna techniques. He received the 2015 IEEE ComSoc Asia Pacific Outstanding Paper Award, the Outstanding Teaching Award from Yonsei, the Motorola Partnerships in Research Grant, the University Continuing Fellowship from UT Austin, and the Best Paper Award from the IEEE GLOBECOM 2006 and PolyU AMA in 2013. He frequently serves on the technical program committees of major IEEE conferences in wireless communications. Most recently, he served as the Lead Chair of the Wireless Communication Symposium of the IEEE Globecom 2017 and the Communication Theory Symposium of the IEEE GLOBECOM 2014 and the TPC Co-Chair of the IEEE PIMRC 2017 and the IEEE CTW 2013. He was an Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Series on Green Communications and Networking from 2015 to 2016, the IEEE WIRELESS COMMUNICATIONS LETTERS from 2011 to 2016, and the IEEE/KICS JOURNAL OF COMMUNICATION AND NETWORKS from 2009 to 2015. He edited the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Special Issue on Communications Powered by Energy Harvesting in 2015. He was an elected member of the SPCOM Technical Committee of the IEEE Signal Processing Society from 2012 to 2015. He is currently an Editor for the newly established IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Yifan Chen (M'06–SM'14) received the B.Eng. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2002 and 2006, respectively. From 2005 to 2007, he was a Project Officer and then a Research Fellow with the Singapore-University of Washington Alliance in bioengineering, supported by the Singapore Agency for Science, Technology and Research, Nanyang Technological University, Singapore, and the University of Washington at Seattle, WA, USA. From 2007 to 2012, he was a Lecturer and then a Senior Lecturer with the University of Greenwich and Newcastle University, U.K. From 2012 to 2016, he was a Professor and the Head of Department of Electrical and Electronic Engineering with the Southern University of Science and Technology, Shenzhen, China, appointed through the Recruitment Program of Global Experts (known as the Thousand Talents Plan). In 2013, he was a Visiting Professor with the Singapore University of Technology and Design, Singapore. He is currently a Professor of Engineering and the Associate Dean External Engagement with the Faculty of Science and Engineering and the Faculty of Computing and Mathematical Sciences, University of Waikato, Hamilton, New Zealand. His current research interests include electromagnetic medical imaging and diagnosis, transient communication with application to healthcare, touchable communication and computation with application to targeted drug delivery and contrast-enhanced medical imaging, fundamentals and applications of nanoscale and molecular communications, and channel modeling for next-generation wireless systems and networks. He is the Coordinator of the European FP7 CoNHealth Project on intelligent medical ICT, an elected Working Group Co-leader of the European COST Action TD1301 MiMed Project on microwave medical imaging, an Advisory Committee Member of the European Horizon 2020 CIRCLE Project on molecular communications, a Voting Member of the IEEE Standards Development Working Group 1906.1 on nanoscale and molecular communications, an Editor for the IEEE ComSoc Best Readings in Nanoscale Communication Networks and the IEEE Access Special Section in Nano-antennas, Nano-transceivers, and Nano-networks/Communications, and a Vice Chair of the IEEE Nano-scale, Molecular and Quantum Networking Emerging Technical Subcommittee.



Rui Wang received the bachelor's degree from the University of Science and Technology of China, in 2004, and the Ph.D. degree in wireless communications from The Hong Kong University of Science and Technology, in 2008. From 2009 to 2012, he was a Senior Research Engineer with Huawei Technologies, Co., Ltd. Since 2012, he has been with the South University of Science and Technology of China, as an Associate Professor. He has research experience in academia and industry. He has authored over 30 papers in top-level IEEE journals and flagship international conferences, especially in the area of wireless radio resource optimization and interference management. He is also involved in the development of interference mitigation technology for 5G systems, and has contributed more than 20 U.S. patent applications and 40 Chinese patent applications (20 of them have been granted).

A New Metric for Measuring the Security of an Environment: The Secrecy Pressure

Lorenzo Mucchi, *Senior Member, IEEE*, Luca Ronga, *Senior Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, Kaibin Huang, *Senior Member, IEEE*, Yifan Chen, *Senior Member, IEEE*, and Rui Wang

***Abstract*— Information-theoretical approaches can ensure security, regardless of the computational power of the attackers. Requirements for the application of this theory are: 1) assuring an advantage over the eavesdropper quality of reception and 2) knowing where the eavesdropper is. The traditional metrics are the secrecy capacity or outage, which are both related to the quality of the legitimate link against the eavesdropper link. Our goal is to define a new metric, which is the characteristic of the security of the surface/environment where the legitimate link is immersed, regardless of the position of the eavesdropping node. The contribution of this paper is twofold: 1) a general framework for the derivation of the secrecy capacity of a surface, which considers all the parameters that influence the secrecy capacity and 2) the definition of a new metric to measure the secrecy of a surface: the secrecy pressure. The metric can be also visualized as a secrecy map, analogously to weather forecast. Different application scenarios are shown: from "forbidden zone" to Gaussian mobility model for the eavesdropper. Moreover, the secrecy outage probability of a surface is derived. This additional metric can measure, which is the secrecy rate supportable by the specific environment.**

***Index Terms*— Physical-layer security, secrecy pressure, secrecy capacity, secrecy outage, security of wireless communications.**

I. Introduction

IN WIRELESS networks, transmission between legitimate nodes can easily be intercepted by an eavesdropper due to the broadcast nature of the wireless medium. This makes wireless transmissions highly vulnerable to eavesdropping attacks. Existing communications systems typically adopt cryptographic techniques in order to achieve confidential transmission, to prevent an eavesdropper from interpreting data transmission between legitimate users.

It is known that encrypted transmission is not perfectly secure, since the cipher text can still be decrypted by an eavesdropper through a brute-force attack, an exhaustive search of the encryption key into the cipher text.

To this end, physical-layer security is an emerging alternative paradigm to protect wireless communications against eavesdropping attacks, including brute-force attacks. In fact, the security of cryptographic techniques is implicitly set into the practical assumption that the attacker does not have enough computational power to hack the cipher text in a reasonable amount of time. Thus, security of encryption algorithm cannot be measured exactly. On the contrary, information-theoretical physical-layer security does not need to make any assumption of the computational power of the attacker, and, in addition, the security of a communication link can be exactly measured.

Physical-layer security work was pioneered by Shannon and evolved by Wyner in [1], where a discrete memoryless wiretap channel was examined for secure communications in the presence of an eavesdropper. Perfectly secure data transmission can be achieved if the channel capacity of the legitimate link is higher than the eavesdropper link (from source to eavesdropper). In [2], Wyners results were extended to Gaussian wiretap channel: a new metric, the secrecy capacity, was proposed. The secrecy capacity was derived as the difference between the channel capacity of the legitimate link and of the eavesdropper link. If the secrecy capacity is above zero, the legitimate source can adapt the data rate in order to let the destination decode the information, while the data overheard by the eavesdropper is too few and noisy to be decoded. If the secrecy capacity falls below zero, the transmission from source to destination becomes completely insecure, and the eavesdropper can succeed in interpreting the data. In order to improve the security against eavesdropping attacks, one solution is to reduce the probability of occurrence of an intercept event through enlarging the secrecy capacity.

As a consequence, there are extensive works aimed at increasing the secrecy capacity of wireless communications by exploiting multiple antennas [3] and/or cooperative relays [4].

A. Related Works

There are some examples in literature of papers attempting to create a physical region to face the randomness of the

Manuscript received September 12, 2016; revised January 20, 2017; accepted February 28, 2017. The work of X. Zhou was supported by the Australian Research Council's Discovery Projects under Grant DP150103905. The work of Y. Chen was supported by the Guangdong Natural Science Funds under Grant 2016A030313640. The associate editor coordinating the review of this paper and approving it for publication was M. Elkashlan.

L. Mucchi is with the Department of Information Engineering, University of Florence, I-50139 Firenze, Italy (e-mail: lorenzo.mucchi@unifi.it).

L. Ronga is with the National Inter-universities Consortium on Telecommunications, University of Firenze research Unit, I-50139 Firenze, Italy (e-mail: luca.ronga@cnit.it).

X. Zhou is with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

K. Huang is with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong (e-mail: huangkb@ieee.org).

Y. Chen is with the Faculty of Science and Engineering, The University of Waikato, Hamilton 3240, New Zealand, also with the Faculty of Computing and Mathematical Sciences, The University of Waikato, Hamilton 3240, New Zealand, and also with the Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen 518055, China (e-mail: yifan.chen@waikato.ac.nz).

R. Wang is with the Department of Electrical and Electronic Engineering, South University of Science and Technology of China, Shenzhen 518055, China (e-mail: wang.r@sustc.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2017.2682245

eavesdropper location and/or the amplitude fluctuation due to fading. All these attempts are basically based on the use of multiple antennas and beamforming [5], [10]–[12]. These works aim at building a region as small as possible where the message can be considered secure. The region is built by using beamforming and/or antenna coding between the legitimate transmitter and receiver, or with the help of friendly surrounding nodes (artificial noise injection, jamming). Actually, the definition of the physical region can differ from paper to paper, but mainly beamforming or jamming are used in the works based on information-theoretical parameters, in the form of antenna arrays [10] or distributed antennas [5].

In [6] secrecy rate maximization and power consumption minimization for a multiple-inputmultiple-output (MIMO) secrecy channel is investigated. A multiantenna cooperative jammer is employed to improve secret communication in the presence of a multiantenna eavesdropper. In [7] and [8] a phase-shifting array is used to produce security in a given direction (directional modulation). The resulting signal is direction-dependent and thus the signal can be purposely distorted in other directions but the desired one. This approach can be used to enhance the security of multiuser multi-input multiple output (MIMO) communication systems when a multiantenna eavesdropper is present [9].

The metric used to measure the security of the legitimate link is always the received signal to noise plus interference ratio (SINR) or the secrecy outage. The metric, such as the secrecy outage, is well known in literature and it is related to the quality of the legitimate link, given the position of transmitter and receiver, the transmit parameters (power, coding, beamforming, etc.), as well as the location of eavesdropping nodes and interference sources. Other papers based on information-theoretical security typically use the metrics such as secrecy capacity or secrecy outage to measure the security level of the legitimate link by supposing to know the positions and the channel state information of the eavesdroppers and interferers. In order to drop out the dependance on the positions of the eavesdropping or interference nodes,[1] a more general secrecy metric which is basically a characteristic of the network topology can be reached by averaging out the secrecy capacity over all the possible positions of eavesdroppers or interferers [13], [14]. Anyway, all the above mentioned papers deal with metrics which express a characteristic of the link, not of the surface where the link is immersed.

B. Our Contribution

The secrecy capacity is a good metric to evaluate how much is secure a single communication link. But in many practical scenarios a metric which is related to the specific environment can be more effective. For this reason we propose and test here a new metric which bonds the secrecy to the surface of the environment. We named this metric *secrecy pressure*, taking an analogy from the weather forecasting. The secrecy pressure is defined as the secrecy capacity insisting over the infinitesimal element of the surface. This metric can be used for several practical scopes: from deriving the secrecy of a specific surface/environment, to calculate which is the optimum transmitting antenna orientation or friendly jammer position.

Differently from traditional metrics such as the conventional secrecy capacity, our metric does not imply to know where Eve is. To be more clear, in our approach the secrecy capacity is calculated for each point (x, y) of a surface S. To do this we suppose that Eve is located in (x, y). Then, we integrate over x and y along the surface S, thus eliminating the dependence on the position of the eavesdropper. The integration operation is, de facto, as taking the average over the space (instead of time). The resulting metric is the secrecy capacity than the entire surface S has got. We call this metric secrecy pressure since it tells how much security insists over a surface S. In other words, we calculate how much secure is an environment, given the position of Alice, Bob and (if present) interferers. It is more practical because 1) we do not have to make any assumptions on the position of the eavesdropper; 2) the new metric is a property of the environment, and not of the point where Eve is located; 3) we calculate a number which gives an insight on how much secure is the environment were going to transmit. The closest concept to this new metric is the network secrecy developed by M. Win *et al.* [13]. The network secrecy is a metric which evaluates the secrecy of an entire network of nodes (not an environment). Legitimate nodes and eavesdropping nodes are randomly distributed as Poisson point processes (PPP). The secrecy capacity is calculated for each legitimate link, given the position of the eavesdroppers. The dependence on the eavesdroppers positions is dropped by averaging out respect to all possible realization of the PPP distribution of the eavesdropper nodes.

The paper also includes a general framework which evaluates the secrecy capacity over a surface. The framework describes all the parameters affecting the secrecy capacity: spatial distribution of the nodes (legitimate and interfering) on a surface, antennas' orientations and patterns, path loss and fast fading statistics of the communication links, transmitting powers. No hypothesis is made over the position of the eavesdroppers, the metric is calculated over the entire surface, as the eavesdropper could be in each point of the surface. Static as well as statistical mobility model are supposed for the eavesdropper. The results show how the metric can be useful in giving an immediate insight on the leakage zones in the surface, and how to adjust the parameters in order to maximize the secrecy. The optimization problem is here formulated for the transmitting antenna orientation and for the position of a friendly jammer.

It is important to highlight that the secrecy pressure does not need to know the position of the eavesdropper (Eve) on the surface of interest. Typically the papers in literature assume to know the position of Eve, which is usually an unpractical assumption. The secrecy pressure or the secrecy map parameters are calculated by assuming that Eve can stay in each point of the surface. If no information about eavesdropper is known, it could be located in any point of the surface with equal probability. We did not introduce a PPP distribution of eavesdropping nodes, although this is a

[1]The eavesdroppers and interferers are supposed to be spatially distributed around the legitimate link with a point poisson process (PPP) distribution.

common approach, since we suppose that Eve can stay in each point of the surface. Typically, the PPP distribution is used to calculate how many eavesdroppers are within the range of the legitimate transmitter, and than average out the secrecy capacity. Our approach is different, we are interested in a new metric which is a characteristic of the surface. Anyway, a PPP distribution for the presence of Eve over the surface can be easily assumed in our case too. The secrecy pressure contains all the parameters that can cause a variation of the secrecy capacity, and thus it can be optimized respect to many (known) parameters (transmit antenna orientation, interference node positions or powers, etc.), separately or jointly.

Another known metric in information-theoretical physical-layer security is the secrecy outage, i.e., the probability that the secrecy capacity is below a target rate. We have derived here the secrecy outage probability of a surface (SOPS). In this case we have supposed that the presence of Eve on the surface is not perfectly known, but it has an uncertain which we have modelled as a Gaussian distribution.

The instant fading coefficient of Eve's channel should be anyway known or estimated in order to derive the secrecy pressure instant by instant. This estimation can be relaxed if the evaluation of the secrecy pressure is done in ergodic channel. The ergodic secrecy pressure can be a useful tool in many practical applications.

Practical applications of the propose metric could be tactical communications: a scenario in which the transmission cannot surely be overheard in a particular zone of the surface. Another scenario could be when the information cannot be leaked along a specific path or street, where the eavesdropper is supposed to move.

The remainder of this article is organized as follows. Sec. II describes the system model; the framework for the evaluation of the secrecy capacity over a surface is introduced, including all the parameters on which it depends, antenna orientation and pattern, nodes position and power, etc. In Sec. III, the new metric called secrecy pressure is defined. Sec. IV proposes the optimization problems, analytical solutions and graphs. In Sec. V some practical application scenarios are considered; antenna orientation as well as friendly jammer problems are solved in specific scenarios: from forbidden zone to mobility of the eavesdropper. In Sec. VI the closed-form of the secrecy outage probability of a surface is derived and discussed. Sec. VII concludes the paper.

II. System Model

Consider a 2D surface S described by Cartesian coordinates (x, y). Into this space there are the legitimate transmitter (node i) and receiver (node j), as well as a given number of interferers I_k with $k = 1, \cdots, N_I$ (Fig. 1). For better comprehension, let's assume that the space is a geographical urban area, the transmitter is a base station, the receiver is a mobile terminal and the interferers are other base stations or access points. We do not assume any specific position for the eavesdropper in the space. In fact, we want to derive how the secrecy is mapped all over the given environment.

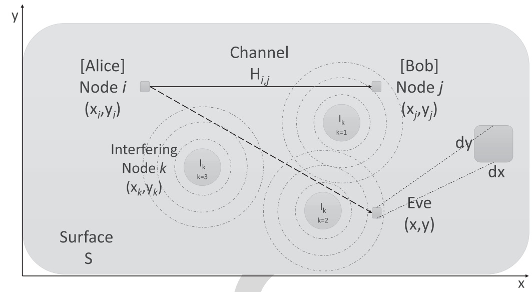


Fig. 1. General scenario. Two legitimate nodes (i and j) want to exchange a confidential message. They are immersed in an environment S together with interfering nodes I_k. The eavesdropper node can be located anywhere over the surface.

A. The Scenario

We assume to have a surface S where Alice and Bob are located and their position is known (Fig. 3). In the environment S there are also interfering nodes, whose positions are also known. Interfering nodes could be intentional jamming sources or simply other systems (base stations) radiating in the same frequency band of the legitimate transmission. To simulate this scenario, the position of Alice and Bob was chosen deterministically, while the position of the interfering nodes were randomly selected, by using a Point Poisson Process (PPP) distribution. The use of a PPP distribution for interfering nodes dispersion around a receiver is common in the literature, when dealing with security of wireless communications. Alice wants to transmit a confidential message M to Bob. The legitimate receiver (Bob) tries to recover the message from the observation vector Z_B. The eavesdropper (Eve) can be located anywhere in the surface S, and tries to recover the message M by analyzing the observation vector Z_E. The wireless channels from Alice to Bob and to Eve are supposed to be statistically independent.

B. Channel Model

Let us suppose to have two nodes on the surface S, a transmitting node i with position (x_i, y_i) and a receiving node j with position (x_j, y_j). The channel between node i and node j is modeled as

$$H_{i,j} = h_{i,j}(\tau, \psi) \cdot d_{i,j}^{-b} \tag{1}$$

where $d_{i,j}$ is the Euclidian distance between the nodes, b is the path loss exponent and $h_{i,j}(\tau, \psi)$ models the multipath fading effect, including angular dispersion

$$h_{i,j}(\tau, \psi) = \sum_{l=1}^{L} h_{i,j}^{(l)} \delta(\tau - \tau_l) \delta(\psi - \psi_j) \tag{2}$$

The parameter τ_l is the delay of arrival of the l-th path, while ψ_l is the angle of arrival of the l-th path, i.e., τ and ψ are modeling the time and angular dispersion of the multiple echoes arriving at the receiver, respectively. The variable $h_{i,j}^{(l)} = a_{i,j}^{(l)} e^{-\beta_{i,j}^{(l)}}$ denotes the channel coefficient, where $a_{i,j}^{(l)}$ is modelled as a stochastic variable with Rayleigh distribution

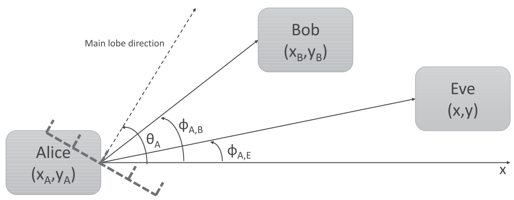


Fig. 2. Antenna pattern of the legitimate transmitter (Alice).

whose probability density function (PDF) is

$$f_{a_{i,j}^{(l)}}(a) = \frac{2a}{\sigma_a} e^{\frac{-a^2}{\sigma_a}}$$

with σ_a representing the standard deviation of the Rayleigh distribution, and $\beta_{i,j}^{(l)}$ is modeled as a stochastic random variable with uniform distribution in $(0, 2\pi)$. Each link that connect two nodes on the surface is supposed to have a fading coefficient which is independent to all others.

C. Received Power

Let us suppose that the node i is transmitting with power P_i. The power received by the node j is

$$P_j = P_i |H_{i,j}|^2 G_i(\theta_i, \phi_{i,j}) G_j(\theta_j, \phi_{j,i}) \tag{3}$$

where $G_i(\theta_i, \phi_{i,j})$ is the antenna pattern gain of the transmitter, $\phi_{i,j}$ is the angle between the x-axis and the segment connecting node i and j, and θ_i is the angle between the x-axis and the direction of maximum radiation (main lobe) of i-node's antenna. Fig. 2 shows the angles mentioned above, when node i is the legitimate transmitter, called Alice, and node j is the legitimate receiver, called Bob.

Defining $\tilde{P}_{i,j} = P_i G_i(\theta_i, \phi_{i,j}) G_j(\theta_j, \phi_{j,i})$ we can rewrite (3) as

$$P_j = \tilde{P}_{i,j} |H_{i,j}|^2 \tag{4}$$

Given the position of node i and j on the surface S, the angles $\phi_{i,j}$ and $\phi_{j,i}$ are fixed. Then, $\tilde{P}_{i,j} = \tilde{P}_{i,j}(\theta_i, \theta_j)$. If, in addition, the receiving node j has isotropic antenna $\theta_j = \text{Const}\ \forall j$, then $\tilde{P}_{i,j} = \tilde{P}_{i,j}(\theta_i)$.

According to [18] and [19], the time dispersion of the multipath at the receiver has an exponential distribution

$$f_\tau(\tau) = \frac{1}{\sigma_\tau} e^{-(\tau - \tau_0)/\sigma_\tau}$$

while the angle dispersion of the multipath at the receiver has a Laplacian distribution

$$f_\psi(\psi) = \frac{1}{\sqrt{2\sigma_\psi^2}} e^{-\sqrt{2}(\psi - \psi_0)/\sigma_\psi}$$

In order to average out the time and angular dispersion, the power P_j has to be integrated over all possible times and angles of arrival

$$\overline{P}_j = \tilde{P}_{i,j} d_{i,j}^{-2b} \int_\tau \int_\psi |h_{i,j}(\tau, \psi)|^2 f_\tau(\tau) f_\psi(\psi) d\tau d\psi \tag{5}$$

D. Aggregate Interference

Let us suppose that the N_I interfering nodes are distributed on the surface S following a point Poisson process (PPP) distribution with density λ. The sum of the interference power at the node j is

$$\begin{aligned} \mathbf{I}_j &= \sum_{k=1}^{N_I} P_k G_k(\theta_k, \phi_{k,j}) G_j(\theta_j, \phi_{j,k}) d_{k,j}^{-2b} |h_{k,j}|^2 \\ &= \sum_k \tilde{P}_{k,j} |H_{k,j}|^2 \end{aligned} \tag{6}$$

where P_k is the power emitted by the k-th interfering node, $d_{k,j}$ is the Euclidian distance between the k-th interfering node and node j and $h_{k,j}$ is the channel coefficient associated to the link (1). If the position of the N_I interfering nodes (x_k, y_k) with $k = 1, \cdots, N_I$ is fixed, then $\tilde{P}_{k,j} = \tilde{P}_{k,j}(\theta_k, \theta_j)$. If, in addition, the receiving node j has isotropic antenna $\theta_j = \text{Const}\ \forall j$, then $\tilde{P}_{k,j} = \tilde{P}_{k,j}(\theta_k)$. In this case, the aggregate interference $\mathbf{I}_j$ is a random variable with Stable distribution [16], [17]

$$\mathbf{I}_j \sim \mathcal{S}(\alpha, 1, \gamma_j) \tag{7}$$

where $\alpha = 1/b$ and

$$\gamma_j = \pi \lambda \Xi_\alpha^{-1} \mathbb{E}\left\{ \left(\sum_k \tilde{P}_{k,j} |h_{k,j}|^2 \right)^\alpha \right\}$$

with

$$\Xi_\alpha = \begin{cases} \dfrac{1-\alpha}{\Gamma(2-\alpha)\cos(\pi\alpha/2)} & \text{if } \alpha \neq 1 \\ \dfrac{2}{\pi} & \text{if } \alpha = 1 \end{cases} \tag{8}$$

where $\Gamma()$ denotes the Gamma distribution function and $\mathbb{E}\{\}$ the expectation operator.

The PDF of $\mathbf{I}_j$ is

$$\begin{aligned} f_{\mathbf{I}_j}(I) &= \frac{1}{2\pi} \int \varphi_I(\omega) e^{-j\omega I} d\omega \\ &= \frac{1}{\pi} \int_0^\infty e^{-\omega^\alpha \gamma_j} \cos\left[\tan\left(\frac{\pi\alpha}{2}\right) \omega^\alpha \gamma_j - \omega I \right] d\omega \end{aligned} \tag{9}$$

where

$$\varphi_I(\omega) = \exp\left\{ -|\omega|^\alpha \left[1 - j\,\mathrm{Sgn}(\omega) \tan\left(\frac{\pi\alpha}{2}\right) \right] \gamma_j \right\}$$

is the characteristic function of the random variable I.

It is important to highlight that depending on the position of the receiver j on the surface S, not all the N_I interferers could affect the receiver. The distance (path loss) $d_{k,j}^{-2b}$ could be close to zero, thus the node k does not contribute to the aggregate interference at the receiver j.

III. Secrecy Pressure and Secrecy Force

We want to define a new metric that allows to measure the intensity of secrecy over a given surface. Taking analogy from the atmospheric weather science, we define the concept of *Secrecy Pressure*.

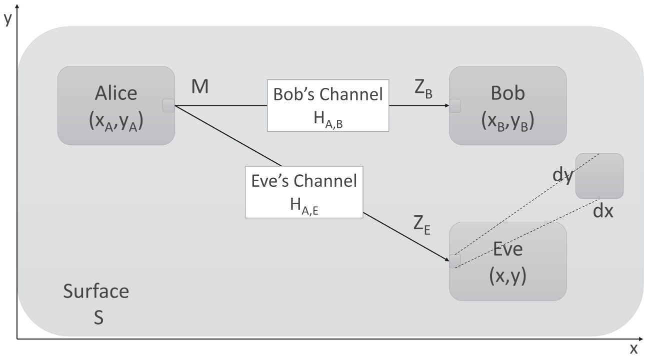


Fig. 3. Scheme of the transmission of the confidential message M from Alice to Bob.

Let us now associate the previous defined transmitting node i as Alice and the receiving node j as Bob. Alice is then located at point (x_A, y_A) and Bob at (x_B, y_B) on the surface S. The position of the eavesdropper Eve is not known, thus we suppose that its coordinates are generically (x, y).

Suppose that Alice wants to transmit a confidential message M to Bob. Bob tries to recover the information M from the vector Z_B received (Fig. 3). Given the model in Sec. II, the mutual information exchanged in the legitimate link (from Alice to Bob) is

$$\mathbb{I}_B = \mathbb{I}(M; Z_B) = \mathbb{H}(M) - \mathbb{H}(M|Z_B) \tag{10}$$

where $\mathbb{H}()$ denotes the entropy.

Analogously, the eavesdropper (Eve) tries to recover the message M from the received vector Z_E. Thus, the information stolen by Eve is

$$\mathbb{I}_E = \mathbb{I}(M; Z_E) = \mathbb{H}(M) - \mathbb{H}(M|Z_E) \tag{11}$$

The term $\mathbb{I}(M; Z_E)$ is called Leakage, and it denotes the amount of information on the message M that Eve is able to recover from the received vector Z_E.

As known, these two mutual information can be used to calculate the secrecy capacity [15]

$$C_{sec} = \max_{\mathfrak{p}_M} \{\mathbb{I}_B - \mathbb{I}_E\} \geq \max_{\mathfrak{p}_M} \mathbb{I}_B - \max_{\mathfrak{p}_M} \mathbb{I}_E = C_B - C_E \tag{12}$$

where C_B and C_E are the capacities of Bob's and Eve's channel, respectively, and $\mathfrak{p}_M$ is the marginal distribution of the codeword M. The secrecy capacity is at least as large as the difference between the legitimate channel capacity and the eavesdroppers channel capacity. The inequality can be strict as in the case of complex Gaussian wiretap channels [15], as well as typical wireless fading channels, which are here considered. It is important to note that both $\mathbb{I}_B$ and $\mathbb{I}_E$ depend on the channel state and position of Bob and Eve respect to Alice, respectively. This means that changing the position of Bob or Eve on the surface S, the mutual information changes.

The capacity of the link between the transmitter, called Alice, positioned in (x_A, y_A), and the position (x_B, y_B) of the legitimate receiver, called Bob, can be written as

$$C_B = \frac{1}{2} \log\left(1 + \frac{P_B}{N_0 + \mathbf{I}_B}\right) \tag{13}$$

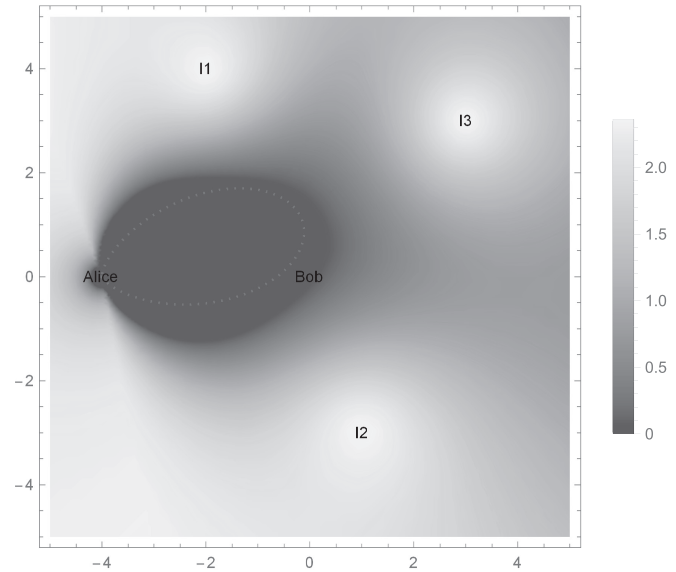


Fig. 4. Secrecy map of surface S with Alice's antenna orientation and pattern. Three interfering nodes (I_1, I_2, I_3) are present. The azimuth of Alice transmission antenna is 6 deg.

where N_0 denotes the Gaussian noise density at the receiver, P_B and $\mathbf{I}_B$ are defined in (4) and (6), respectively.

Since typically we cannot know if an eavesdropper, called Eve, is present in the surface S or where it is located, we derive the capacity of a generic point (x, y) of the surface, i.e.,

$$C_E(x, y) = \frac{1}{2} \log\left(1 + \frac{P_E}{N_0 + \mathbf{I}_E}\right) \tag{14}$$

where P_E and $\mathbf{I}_E$ are defined as in (4) and (6), respectively

$$P_E = P_A G_A(\theta_A, \phi_{A,E}) G_E(\theta_E, \phi_{E,A}) d_{A,E}^{-2b} |h_{A,E}|^2$$

$$\mathbf{I}_E = \sum_{k=1}^{N_I} P_k G_k(\theta_k, \phi_{k,E}) G_E(\theta_E, \phi_{E,k}) d_{k,E}^{-2b} |h_{k,E}|^2$$

Thus, supposing that Eve is located in a generic point (x, y) on the surface S, the secrecy capacity of the link between Alice and Bob is

$$C_{sec}(x, y) = \max\{0, C_B - C_E(x, y)\} = [C_B - C_E(x, y)]^+ \tag{15}$$

It is important to highlight that the capacities here are intended as conditioned to the state of the channels $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$, as well as the state of the aggregate interference $\mathbf{I}_B$ and $\mathbf{I}_E$.

What we are proposing here is to define a secrecy capacity for each elementary point (x, y) of the surface S. Using this representation, we can elaborate a map of the secrecy of the surface given the position of the known actors, i.e., legitimate users and interfering nodes. In other words, given the positions of Alice, Bob and interfering nodes I_k, for each point (x, y) of the surface, we calculate the secrecy capacity of the legitimate link as Eve was located in that point. The result is that we can draw a map showing the different levels of secrecy of the entire surface S (Fig. 4).

The *Secrecy Pressure* p_{sec} is defined as

$$p_{sec} = \frac{1}{A_S} \iint_S C_{sec}(x,y)dxdy = \frac{F_{sec}}{A_S} \tag{16}$$

where A_S denotes the area of the surface S and the term F_{sec} is denoting what we define as *Secrecy Force*. The secrecy force depends on the locations of the legitimate users and interfering nodes, but not on the eavesdroppers. The metric p_{sec} is a useful parameter that indicates how much is secure a surface S, given the position of legitimate nodes and interfering nodes. Using this metric, different surfaces and/or nodes configurations can be thus ordered

$$p_{sec}^{(1)} < p_{sec}^{(2)} < p_{sec}^{(3)} < \cdots$$

The index allows a ranking of a given spatial configuration of legitimate entities and interferes.

Detailing Eq. (16), we can find an interesting property of the secrecy pressure

$$p_{sec} = \frac{1}{A_S} \int_x \int_y \begin{cases} 0 & \text{if } C_B \le C_E(x,y) \\ C_B - C_E(x,y) & \text{if } C_B > C_E(x,y) \end{cases} dxdy \tag{17}$$

Since C_B does not depend on (x, y), if the surface goes to infinity, the secrecy pressure tends to a constant value

$$\lim_{S\to\infty} p_{sec} = \lim_{S\to\infty} \left(\frac{1}{A_S} \iint_S [C_B - C_E(x,y)]^+ dxdy \right) = C_B \tag{18}$$

This is because the path loss component $d_{A,E}^{-2b}(x,y)$ in (3) vanishes as the generic point (x, y) on the surface S goes to infinity. In practice, the contributions that decrease the secrecy pressure mainly comes from the points on the surface close to the legitimate link. In other words, supposing to have an infinite surface, the set of points where Eve could be located that influence the secrecy capacity is limited, due to the path-loss. A point (x, y) too far away from the legitimate nodes cannot affect the secrecy capacity, since the legitimate signal is received with a too low power to observe anything ($C_E(x, y) = 0$).

From Eq. (15) we can derive another useful representation, called *Secrecy Map*. The $C_{sec}(x, y)$ in (15) is indicating which is the secrecy capacity insisting over the elementary unit surface $dxdy$ located in a generic point (x, y) of the surface S (see Fig. 3). This representation can be used to draw the behaviour of the secrecy capacity over the surface S, showing zones where the secrecy is low or high, analogously to the weather forecast (Fig. 4). The map, in fact, is built by calculating the secrecy capacity of the legitimate link as the eavesdropper was located in each point of the surface. The blue zones in Fig. 4 indicate no secrecy, i.e., if the eavesdropper is set there, the secrecy rate of the legitimate link is zero. Summarizing, the secrecy map is derived by the following steps:

1) take a surface with cartesian coordinates;
2) locate the legitimate nodes (Alice and Bob) on the surface;
3) compute the secrecy capacity of the legitimate link assuming that Eve is located in a point (x,y) of the surface;
4) associate that secrecy capacity to the corresponding point of the surface;
5) repeat 3 and 4 for every point of the surface.

The secrecy capacity associated to a generic point of the surface could be zero, i.e., any time Eve has a greater channel capacity compared to Bob.

The secrecy map of the surface S changes with

- the positions of Alice, Bob and interfering nodes I_k ($k = 1, \cdots, N_I$);
- the pattern and the orientation $G_A(\theta_A)$ of the legitimate transmitter antenna;
- the power of the legitimate transmitter P_A;
- the power of the transmitters of the interfering nodes P_k;
- the state $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$ of the channels.

The effect of time and angle dispersion at the receivers can be averaged out by replacing $\overline{P}_j$ with $j = B$ in (13) and with $j = E$ in (14).

As listed in the above items, the secrecy capacity in (15) depends on the instant fading coefficients $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$. This means that the secrecy pressure (16) (and the secrecy map) depends instantly on these processes. In order to remove the dependance on the instantaneous realizations of the fading coefficients, two solutions can be run: 1) put the characteristic function of the fading coefficients into the secrecy capacity formula and average it out, or more easily, 2) assume that the channels are ergodic. The results shown in this paper are calculated by supposing ergodic channels. Ergodic-fading model characterizes a situation in which the duration of a coherence interval is on the order of the time required to send a single symbol. The processes $h_{A,B}$, $h_{A,E}$, $h_{k,B}$ and $h_{k,E}$ are mutually independent and i.i.d.; fading coefficients change at every channel use and a symbol experiences many fading realizations.

The ergodic secrecy capacity is thus [15]

$$\widetilde{C}_{sec}(x,y) = \mathbb{E}_{|h_{A,B}|^2,|h_{A,E}|^2,|h_{k,B}|^2,|h_{k,E}|^2} \left\{ [C_B - C_E(x,y)]^+ \right\} \quad k = 1, \cdots, N_I \tag{19}$$

where the operator $\mathbb{E}\{\}$ stands for the expectation. The ergodic secrecy pressure is obtained by substituting the ergodic secrecy capacity in (19) into Eq. (16)

$$\widetilde{p}_{sec} = \frac{1}{A_S} \iint_S \widetilde{C}_{sec}(x,y)dxdy \tag{20}$$

Since $\widetilde{C}_{sec}(x, y)$ could be zero in some points of the surface, computing $\widetilde{p}_{sec}$ implies to make an integral of an irregular function.

It is important to point out that the power received by Eve depends on the position of Eve, since path-loss, fading, angle-of-departure, angle-of-arrival, as well as the power of the aggregate interference are position-dependent parameters. Therefore, in the expression of the capacity of both Bob and Eve, the parameters are position-dependent. Since we want a metric which is not dependent on the position of Eve (its position is not known with 100% probability, typically),

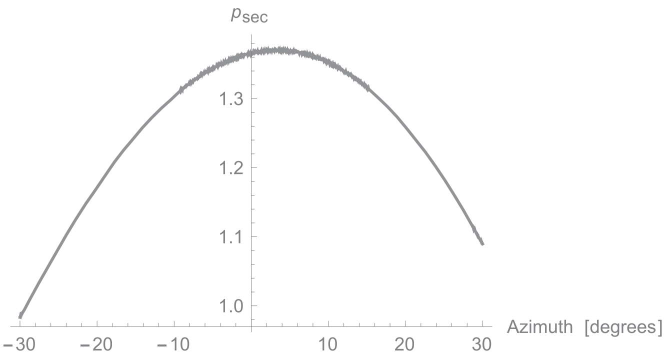


Fig. 5. Secrecy pressure when the optimization problem is solved respect to Alice's antenna orientation.

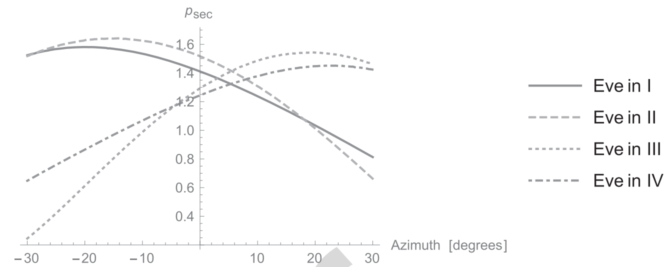


Fig. 6. Secrecy map for different positions of Eve (I, II, III and IV quadrant) when the optimization problem is solved respect to Alice's antenna orientation.

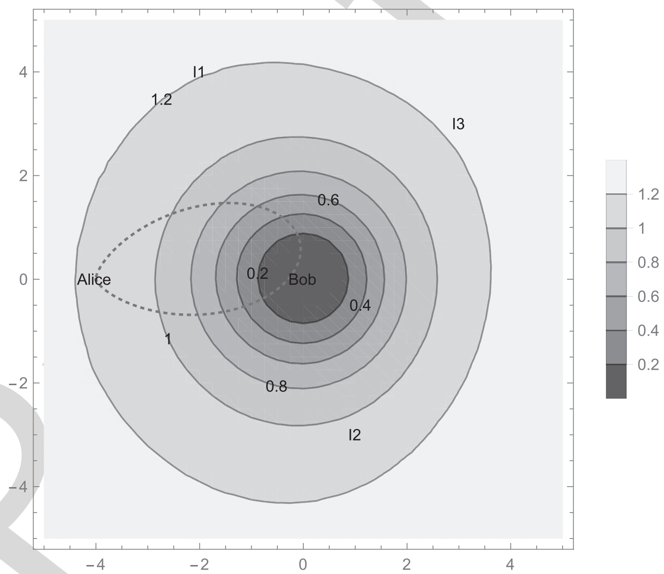


Fig. 7. Secrecy map over the surface S when the optimization problem is solved respect to the position of the additional interfering node (flasher).

we first locate Eve in each point (x,y) of the surface S, we calculate the secrecy capacity of each point (x,y) and then we integrate over the entire surface S. In this way, we take the mean over a space of the secrecy capacity, which eliminates the dependence of the secrecy capacity by specific position of Eve. The resulting (new) metric is a characteristic of the surface and not of the link, thus we called it secrecy pressure.

IV. Secrecy Optimization

The secrecy pressure can be used as a useful metric to determine which is the best configuration parameters to optimize the secrecy of a link. The proposed metric is suitable to find out different useful results, such as: a) which is the antenna orientation that assures highest secrecy towards the legitimate receiver; b) where is the best location where to put additional interfering node(s) in order to reach higher secrecy for the legitimate link; c) which is the best configuration of power emissions from the interfering nodes in order to have highest secrecy for the legitimate link.

A. Antenna Orientation

Let us suppose for simplicity that the interfering nodes I_k as well as Bob and Eve have isotropic antennas. Fixed the surface S, the positions of the legitimate nodes (Alice, Bob) and of the interfering nodes I_k ($k = 1, \cdots, N_I$), and given the pattern of the transmitting antenna $G_A(\theta_A)$, we can maximize the secrecy pressure respect to the antenna orientation

$$\arg\max_{\theta_A} \{p_{sec}\} \tag{21}$$

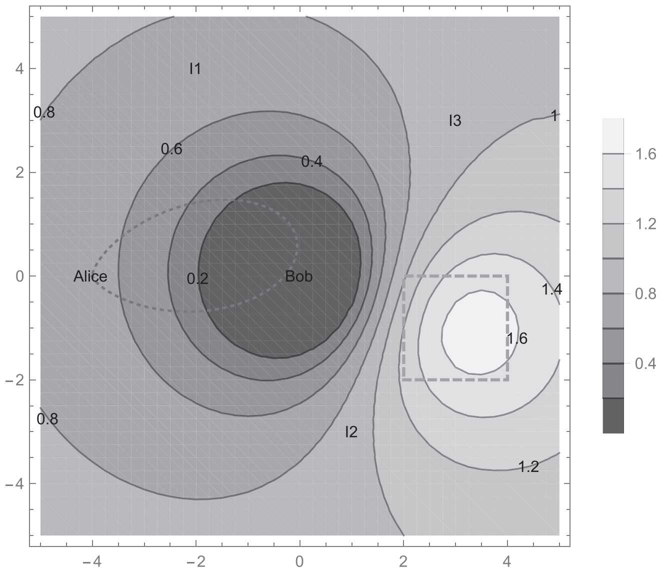
Fig. 5 shows the secrecy map over the surface S when Eve is supposed to be set somewhere in the surface S and the optimization problem is solved respect to Alice's antenna orientation. There exists an optimum azimuth orientation of Alice's antenna. Given the positions of the legitimate users and interfering nodes, the best, from the secrecy capacity point of view, for Alice is not to point the maximum of the antenna pattern towards the direction of Bob. An azimuth orientation of +6 deg optimizes the secrecy capacity, in this case. In general, with the proposed metric it is possible to derive easily which is the best antenna orientation for the transmission to a legitimate receiver in a given perimeter, of which we know only the positions of the interferers (e.g., other access points or base stations). Fig. 6 shows the secrecy map over the surface S for different positions of Eve (I, II, III and IV quadrant) when the optimization problem is solved respect to Alice's antenna orientation. As an example, suppose that the legitimate users do want to minimize the information leakage in a specific zone of the surface (e.g., the eavesdropper is suspected to be in the third quadrant), then the optimum antenna orientation for Alice is +16 deg (green curve in Fig. 6).

B. Interfering Node Positions

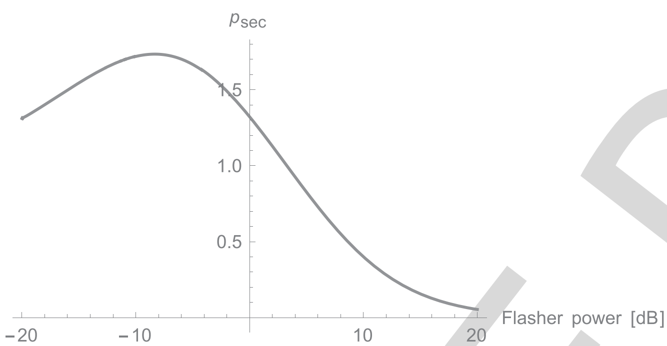
Fixed the surface S, the positions of the legitimate nodes (Alice, Bob) and given the pattern and orientation of the transmitting antenna $G_A(\theta_A)$, we can maximize the secrecy pressure over the position (x_k, y_k) of the $N_I + 1$-th interfering node, a friendly jammer called here *flasher*, in order to maximize the secrecy pressure of the legitimate link, given the positions (fixed) of the N_I interfering nodes

$$\arg \max_{(x_k, y_k),\ k=N_I+1} \{p_{sec}\} \tag{22}$$

Fig. 7 shows the secrecy map over the surface S when the optimization problem (22) is solved. As it can be seen, there are positions where the additional interference node (flasher)



(a) Secrecy map over the surface S when the optimization problem is solved respect to the position of the additional interfering node (flasher). Eve is supposed to be somewhere in the green dotted line.



(b) Secrecy pressure as a function of the power of the additional interfering node (flasher). The flasher is supposed to be placed in the center of the lighter zone depicted in Fig. 8(a).

Fig. 8. Optimization of both position and power of the additional interfering node (flasher).

can be put which optimize the secrecy pressure metric. Like forecast weather, the areas with same color bring the same secrecy capacity, if the additional interfering node (friendly jammer) is installed in that point of the surface. Another evident result is that the interfering node cannot be placed close to Bob (white hole in Fig. 7), since the this would decrease drastically the capacity of the legitimate link and thus the secrecy capacity. Fig. 8(a) shows the same secrecy map in the case that Eve is supposed to be somewhere in a limited perimeter (the green dotted line) inside the surface S. In this case the optimum area is modified compared to the previous scenario.

C. Power Allocation of the Interferers

Fixed the surface S, the positions of the legitimate nodes (Alice, Bob) and of the interfering nodes[2] I_k, and given the pattern and orientation of the transmitting antenna $G_A(\theta_A)$, we can maximize the secrecy pressure respect to the power emitted by the interfering nodes

$$\arg\max_{P_k} \{p_{sec}\} \quad k = 1, \cdots, N_I \tag{23}$$

To ease the illustration of this optimization, let us suppose to put an additional interfering node (the 4th) in the scenario and to optimize its transmit power. Figs. 8(a) shows the secrecy map over the surface S when the optimization problem is solved respect to the position of the additional interfering node (flasher) and its power. The eavesdropper is supposed to be located somewhere in a limited perimeter (the green dotted line in the figure) of the surface. The lighter zone of the secrecy map denotes the set of points (x,y) where the flasher can be located to yield the highest secrecy pressure. Fig. 8(b) shows the secrecy pressure as a function of the power of the flasher. The curve evidently shows an optimum point, which in that case is about −9 dB.

It is important to stress that using the proposed metric the optimum antenna orientation is not trivially in the direction of the legitimate receiver, as well as the optimum position and power of the intentional jammer (flasher) are not those that the common sense would suggest.

D. Joint Optimization

Joint optimization of all the parameters (antenna orientation, friendly jammer position and interfering power allocation) is also possible

$$\arg\max_{(\theta;(x_k,y_k);P_k)} \{p_{sec}\} \quad k = 1, \cdots, N_I \tag{24}$$

Graphical results of this optimization are not shown in this paper due to the lack of space.

E. Varying the Position of Bob

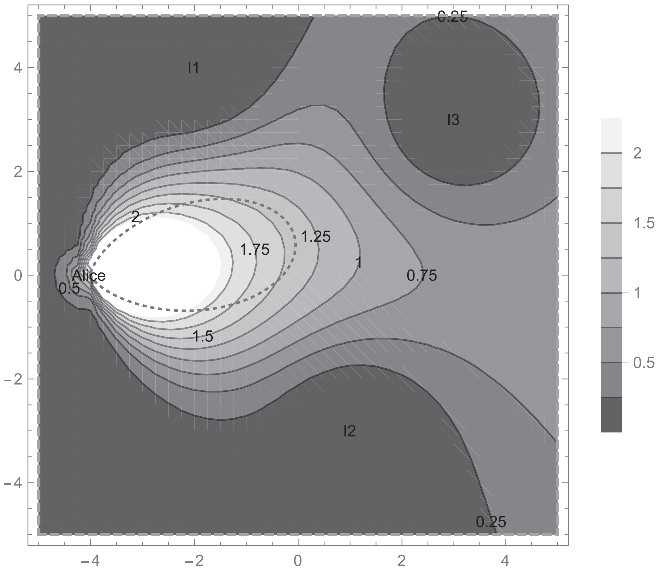
Although the most practical scenario is when Alice and Bob are fixed and Eve can be everywhere in a limited space, as previously described, one could also be interested in using the proposed metric to draw the map of the secrecy pressure when Bob's position can vary over the surface S. In this case, the steps to draw the map are the following

- locate the legitimate receiver (Bob) in a point (x, y) of the surface S;
- calculate the secrecy pressure metric (20) for Bob located in that point;
- assign to the point (x, y) the value of the secrecy pressure;
- repeat these points until all the surface S is evaluated.

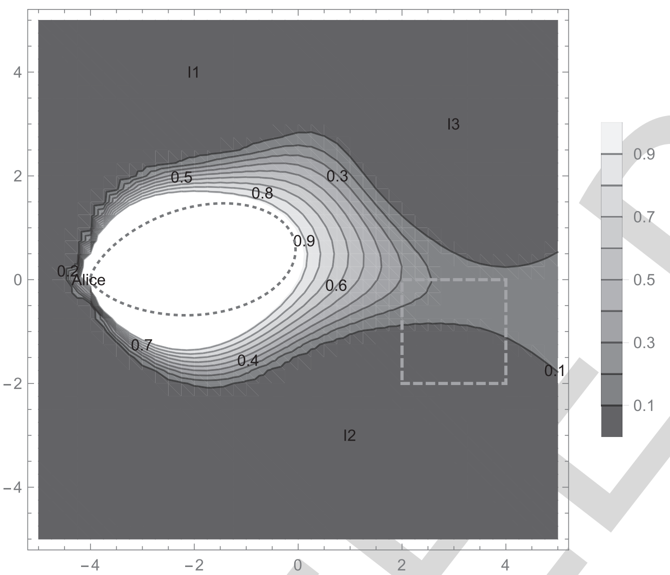
Fig 9(a) shows the map of the secrecy pressure when Bob's position varies over the surface and Eve's position varies over the entire surface as well. As expected the secrecy pressure is higher when Bob is inside the main lobe of Alice, while the secrecy pressure decreases drastically when Bob is closer to an interferer.

Fig 9(b) shows the map of the secrecy pressure when Bob's position vary over the surface and Eve's position varies only in a limited perimeter (the green dashed line). Compared to Fig 9(a), if Eve is confined into a limited space in

[2]The position of the interfering nodes has been randomly selected by using a PPP distribution.



(a) Map of the secrecy pressure as a function of Bob's position. Eve can be everywhere over the surface.



(b) Map of the secrecy pressure as a function of Bob's position. Eve is supposed to be somewhere in the green dotted line.

Fig. 9. Map of the secrecy pressure. The secrecy pressure is calculated as Bob was in each point (x, y) of the surface S.

the surface S, the zone of maximum secrecy pressure is larger and located around the main lobe of Alice. Please note that the secrecy pressure behind Alice, e.g. the point $(-4, -2)$, is low since there is almost no power from Alice in that direction.

V. General Definition of Secrecy Pressure and Practical Applications

As stated in the previous sections, the new metric is defined starting from the definition of the well-known secrecy capacity (C_{sec}). To eliminate the dependence on the position of the eavesdropper of the secrecy capacity, we have averaged out the secrecy capacity by integrating the C_{sec} over the 2D-space of the specific surface S. The resulting metric is called secrecy pressure and it is the analytical expression of the average over a space (instead of time). The integral of the C_{sec} function is not easy to derive, since C_{sec} shows sparsely zeros over the 2D surface, each time that the capacity of Eve is greater of the capacity of Bob. A closed-form expression of the secrecy pressure is not easy to obtain, even for simple geometry shape like circle or square with generic boundaries. For this reason, we have derived the closed-form expression of the secrecy outage of a surface (see Sec. VI). Although a closed-form expression of the secrecy pressure for a known shape is not shown in the paper, this does not mean that the metric makes no sense. The metric is defined as the spatial average of the secrecy capacity calculated for every point of the surface S. The average of the secrecy capacity over time is called ergodic secrecy capacity in the literature, but no previous paper, in our knowledge, presented the spatial average.

This metric shows the secrecy as a characteristic of a surface and not of a single link. This is useful in many practical scenarios, like military tactical scenarios. Typically, military command has a specific perimeter of operation, where the presence of the enemy is not perfectly known, based on the information that the intelligence service or technologies (satellite, etc.) can collect. Most probably, the military command can delimit the presence of the enemy in some zones of the operational scenario, associating the presence of the enemy with a certain probability. By calculating the secrecy pressure, the military command can: 1) quantify how much secure is one perimeter from the point of view of the wireless transmissions; 2) decide the optimum angle for the transmitting antenna array; 3) decide which is the optimum position to place a jammer to enhance the security of the transmission; 4) decide the optimum power of the jammer, in order not to degrade the reception of the legitimate receiver while jamming the potential eavesdropper; 5) operate a multi-parameter optimization; 6) if the position of the eavesdropper is only partially known, the military command can draw zones in the operational perimeter giving to each of them a statistical probability of Eve presence, and then compute the secrecy of the perimeter; 7) if a mobility model of Eve is known or partially (statistically) known, again all the above mentioned parameters (antenna orientation, friendly jammer position, etc.) can be optimized. Other optimizations can be further imagined.

As discussed above, in many practical situations we do not know if an eavesdropper is present and where it is located exactly. Thus, we define a probability of presence of Eve to be associated to a generic point (x, y) on the surface S

$$\Upsilon_{X,Y}(x, y) = Prob\{x \leq X \leq x + dx,\ \ y \leq Y \leq y + dy\}$$
$$= \int_{x}^{x+dx} \int_{y}^{y+dy} \upsilon_{X,Y}(x, y) dx dy \qquad (25)$$

where $\upsilon_{X,Y}(x, y)$ is the probability density function (PDF) of the presence of Eve in (x, y). From now on we call this PDF $\upsilon_E(x, y)$.

The secrecy pressure is thus re-defined as follows

$$p_{sec} = \iint_S \upsilon_E(x, y) C_{sec}(x, y) dx dy \qquad (26)$$

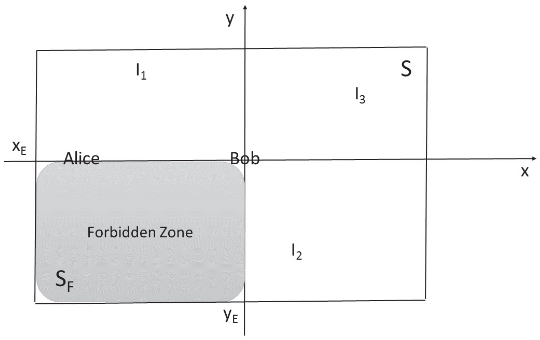


Fig. 10. Forbidden zone inside the surface S.

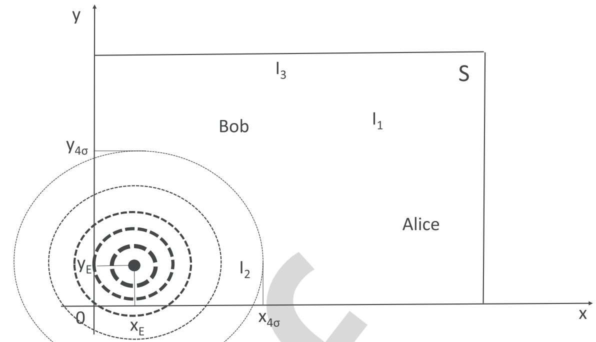


Fig. 11. Gaussian distribution of Eve's presence inside the surface S.

where $C_{sec}(x,y) = [C_B - C_E(x,y)]^+$ and $\iint \upsilon_E(x,y)\, dxdy = 1$. Eq. (26) represents the more general expression of the secrecy pressure in (16). For example, if a uniform distribution of Eve's presence is supposed for the entire surface S, the PDF would be $\upsilon_E(x,y) = 1/A_S$ and thus $\iint_S 1/A_S dxdy = 1$.

In the following sections three practical scenarios are proposed to show the benefits of the new proposed metric. In particular, the secrecy pressure is computed when

- an eavesdropper is known to be in a sub-region of the surface S (leakage zone),
- the eavesdropper position is known with a probability spatial function (Gaussian approximation), and
- when the eavesdropper has not a fixed position (mobility scenario).

In all these cases, some simplifications are assumed

- the average fading of the channels is supposed to be 1, i.e., $\sum_l |h_{i,j}^{(l)}|^2 = 1$;
- the antenna pattern of Bob, Eve and of the interfering nodes is supposed to be isotropic. Only Alice has a directive antenna and can modify the antenna orientation;
- the position of Alice and Bob on the surface S is supposed to be fixed and known: $(-4,0)$ and $(0,0)$, respectively;
- the position of the interfering nodes (I_1,I_2,I_3) is supposed to be fixed and known: $(-2,4)$, $(1,-3)$ and $(3,3)$, respectively.

A. Leakage Zone

In many real situations, e.g., in military scenarios, the transmitter does not want to leak information in fixed zone, in a region where it knows that an eavesdropper is surely present. We name here the leakage zone as *forbidden zone*, since the legitimate transmitter surely does not want to leak any information in that zone. Fig. 10 shows the surface S with the forbidden zone S_F inside. In this example the forbidden zone is the third quadrant.

To each point of the surface S_F we associate a probability of Eve's presence such that $\iint_{S_F} \upsilon_E(S)dxdy = 1$, while in the rest of the surface S we set $\iint_{\neg S_F} \upsilon_E(S)dxdy = 0$, where $\neg S_F$ denotes the complementary surface $S_F \cup \neg S_F = S$.

Assume, as an example, to have an equal distribution of the probability of Eve's presence in the surface S_F. Than,

$$\upsilon_E(x,y) = \begin{cases} \dfrac{1}{x_E y_E}, & \text{if } x \in [0, x_E] \text{ and } y \in [0, y_E] \\ 0, & \text{otherwise} \end{cases} \tag{27}$$

In this case the secrecy pressure of the surface (26) is

$$p_{sec} = \int_0^{x_E}\int_0^{y_E} \upsilon_E(x,y) C_{sec}(x,y)dxdy \tag{28}$$

The secrecy map of the surface can be drawn by using the following result

$$\upsilon_E(x,y)C_{sec}(x,y)$$
$$= \begin{cases} 0 & \text{if } C_{sec}(x,y) = 0 \\ C_B - \dfrac{1}{x_E y_E}\int_0^{x_E}\int_0^{y_E} C_E(x,y)dxdy & \text{otherwise} \end{cases} \tag{29}$$

The optimization of the secrecy pressure respect to the azimuth of the transmitting antenna of the legitimate node (Alice) for a forbidden zone is shown in Fig. 5.

B. Gaussian Probability of Eavesdropper Presence

In other situations, it is not known exactly if eavesdroppers are present or not. Only suspicious. In this case, located a point on the map, a probability of presence of Eve with certain distribution can be associated. We suppose here that a Gaussian spatial distribution of Eve's presence is associated to a zone of the surface S. To each point of the surface S we associate a probability of Eve's presence υ_E which is a random variable with Gaussian distribution centered in (x_E, y_E) (Fig. 11). The circle lines denotes the intensity of the probability. For example, if the Gaussian random variable denoting the presence of Eve on the surface has mean 0.8 and variance 1, we associate a probability of Eve's presence equal to 0.8 to the point (x_E, y_E).

In this case the secrecy pressure of the surface (26) is

$$p_{sec} = \iint_S \upsilon_E(x,y)C_{sec}(x,y)dxdy \tag{30}$$

With $\upsilon_E(x,y) = \frac{1}{\sqrt{2\sigma_E^2}} e^{\frac{(x-x_E)^2+(y-y_E)^2}{2\sigma_E}}$, where σ_E indicates the standard deviation of the Gaussian distribution.

The secrecy map of the surface can be drawn by using the following result

$$\upsilon_E(x,y)C_{sec}(x,y)dxdy = \begin{cases} 0 & \text{if } C_{sec}(x,y) \le 0 \\ C_B - \iint_S \upsilon_E(x,y)C_E(x,y)dxdy & \text{otherwise} \end{cases} \tag{31}$$

This scenario is a particular case of the mobility scenario described in the next section, the results can be appreciated in Fig. 13(b).

C. Mobility Model for the Eavesdropper

If we know the position of Eve at time t_n, we can associate to the eavesdropper a statistical mobility model and derive the secrecy pressure over a surface of interest. The mobility model for Eve depends on its movement capability in the specific environment. In the absence of prior information on the real movement of the eavesdropper (i.e., Eve is free to move in all directions with different speeds), the Gaussian mobility model represents a fairly general model with a tractable number of parameters. In the presence of some prior information on the eavesdroppers movement (e.g., direction or speed is set by the environment), a mobility model more tight to the real mobility would provide better performance.

Optimization of the secrecy pressure is shown respect to the azimuth of the legitimate transmitting antenna as well as respect to the position of the flasher.

We consider here Gaussian mobility model with conditional PDF of current position conditioned on the previous position. For easier notation, let us define the position (x, y) at time t_n of a point on the surface S as a vector $\mathbf{p}_n$. Thus, the conditional PDF of current position is

$$\upsilon_m(\mathbf{p}_n|\mathbf{p}_{n-1}) = \frac{1}{2\pi|\Sigma_m|^{\frac{1}{2}}} e^{-\frac{1}{2}\left[(\mathbf{p}_n-\boldsymbol{\mu}_n)^T \Sigma_m^{-1}(\mathbf{p}_n-\boldsymbol{\mu}_n)\right]} \tag{32}$$

where $\boldsymbol{\mu}_n$ varies with the mobility model as described in the following, and the covariance matrix Σ_m accounts for the uncertainty in the movements in a 2-D plane; thus, it is expressed by

$$\Sigma_m = \begin{bmatrix} \sigma_{m,x} & \rho\sigma_{m,x}\sigma_{m,y} \\ \rho\sigma_{m,x}\sigma_{m,y} & \sigma_{m,y} \end{bmatrix} \tag{33}$$

where $\sigma_{m,x}$ and $\sigma_{m,y}$ is the standard deviation along the x and y axes, respectively. The parameter ρ takes into account the possible inter-dependence of the two coordinates. Independent coordinates have $\rho = 0$.

The mean $\boldsymbol{\mu}_n$ depends on the position $\mathbf{p}_{n-1}$ and the speed $\mathbf{v}_{n-1}$ according to

$$\boldsymbol{\mu}_n = \mathbf{p}_{n-1} + \mathbf{v}_{n-1}(t_n - t_{n-1}) \tag{34}$$

where $\mathbf{v}_{n-1}$ is the vector of the speed along x and y axes at time t_{n-1}.

Fig. 12 shows the secrecy map over the surface S as a function of the position of the flasher (22) and with mobility model for the eavesdropper (32). Eve is suspected to move vertically from its previous position, with a mobility model given by (32). The interfering nodes I_1, I_2 and I_3 are fixed.

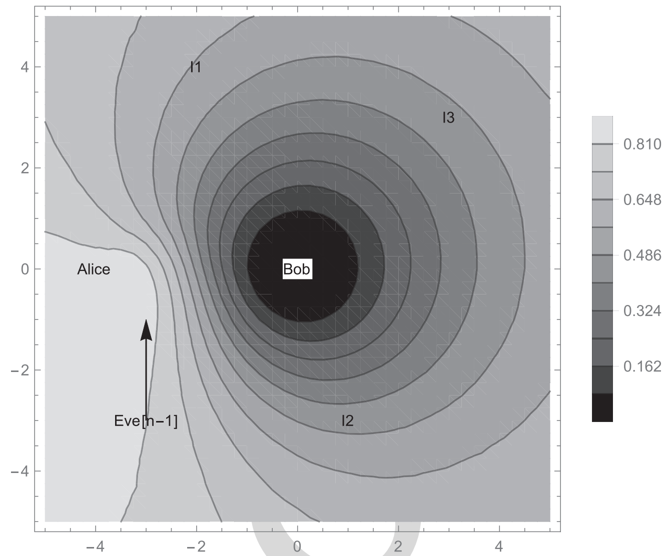


Fig. 12. Secrecy map of the position of the flasher with mobility model for the eavesdropper.

Solving (22) gives the optimum point where to locate the additional flasher I_4. Best is to put the flasher close to the point where the eavesdropper is supposed to arrive. This is somehow trivial.

In order to complicate the scenario we supposed that Eve is moving from $(3, -3)$ to $(3, 3)$ with a mobility model given by (32) (see Fig. 13(a)) in six time steps. Alice antenna azimuth orientation can vary from -30 to $+30$ deg. The resulting map of the secrecy pressure is shown in Fig. 13(b). The map shows which is the optimum transmit antenna orientation (azimuth) at each time step. As an example, at time step 6, Eve is stochastically supposed to be in $(3, 3)$ and thus an orientation between -18 to $+8$ deg optimizes the secrecy capacity for the Eve's mobility scenario. In this case the secrecy rate achievable is more than 3.20 bps. On the contrary, at time step 3 the maximum secrecy rate achievable is 1.28 bps with an antenna orientation range of $(-26, -20)$ deg.

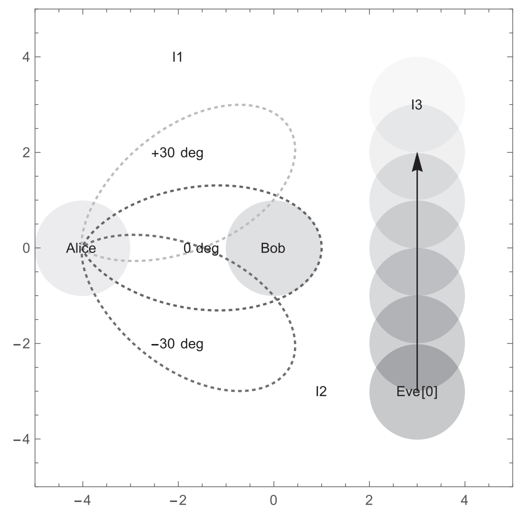
VI. Secrecy Outage Probability of a Surface (SOPS)

A closed-form of the secrecy pressure is not easy to be derived. Another interesting metric could be the outage probability of the secrecy capacity over a surface. A secure outage occurs when the instantaneous secrecy capacity $C_{sec}(x, y)$ is less than target secrecy rate $\overline{R}_{sec}$. Thus, the secure outage probability is defined as

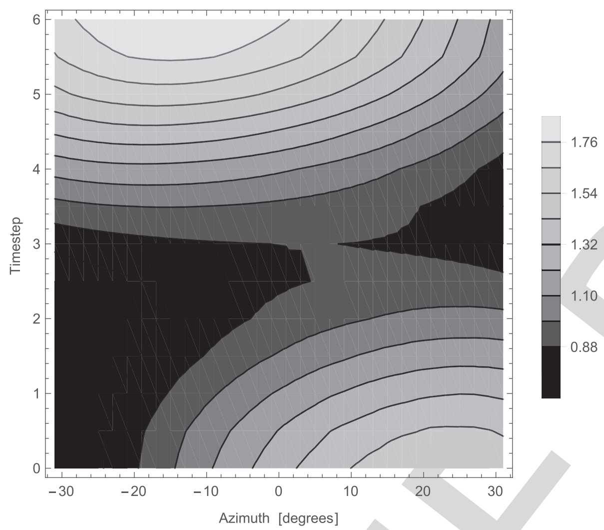
$$P_{out}(\overline{R}_{sec})(x, y) = \text{Prob}\{C_{sec}(x, y) < \overline{R}_{sec}\} \tag{35}$$

Note that the outage probability depends on the location (x, y) of the eavesdropper over the surface. Given the result above, we define the secrecy outage probability of a surface S (SOPS) as

$$A_{out}(\overline{R}_{sec}) = \iint_S P_{out}(\overline{R}_{sec})(x, y)\upsilon_E(x, y)dxdy = \iint_S \text{Prob}\{C_{sec}(x, y) < \overline{R}_{sec}\upsilon_E(x, y)dxdy \tag{36}$$



(a) Eve's mobility scenario.



(b) Secrecy map of the Alice's antenna orientation with mobility model for the eavesdropper.

Fig. 13. Eve's mobility: scenario description and secrecy map over azimuth of Alice's antenna.

The secrecy outage probability of a surface depends on the probability $\upsilon_E(x, y)$ that Eve is located in the point a generic point (x, y) of the surface. An interesting behaviour to study is the existence of the secrecy capacity over a surface, i.e., when $\overline{R}_{sec}$ is set to zero. In this case the SOPS becomes

$$A_{out}(\overline{R}_{sec} = 0) = \iint_S \text{Prob}\{C_{sec}(x, y) = 0\} \upsilon_E(x, y) dx dy \tag{37}$$

The term $\upsilon_E(x, y)$ is the distribution of the presence of Eve over the surface, which could be uniform or Gaussian or any other distribution, based on what it is known about the eavesdroppers. The term $\text{Prob}\{C_{sec}(x, y) = 0\}$ can be derived as

$$\text{Prob}\{C_{sec}(x, y) = 0\} = \text{Prob}\{SNR_E(x, y) \geq SNR_B\} \tag{38}$$

where

$$SNR_B = \frac{P_B}{N_0 + \mathbf{I}_B} \tag{39}$$

$$SNR_E(x, y) = \frac{P_E}{N_0 + \mathbf{I}_E} \tag{40}$$

with P_B, P_E defined as in (3) and $\mathbf{I}_B$, $\mathbf{I}_E$ as in (6). Eq. (38) is hard to be calculated analytically, since the term at numerator P_B is Rayleigh distributed, while the term at the denominator $\mathbf{I}_B$ is Stable distributed. A closed form can be reached if we assume that the Gaussian approximation is valid for the aggregate interference, i.e., $\mathbf{I}_B \sim \mathcal{N}(0, N_B)$ and $\mathbf{I}_E \sim \mathcal{N}(0, N_E)$. In this case Eq. (41) becomes

$$SNR_B = \frac{P_B}{N_0 + N_B} \tag{41}$$

$$SNR_E(x, y) = \frac{P_E}{N_0 + N_E} \tag{42}$$

and Eq. (38) can be written as [20]

$$\begin{aligned} \text{Prob}\{C_{sec}(x, y) = 0\} &= \text{Prob}\{SNR_E(x, y) \geq SNR_B\} \\ &= \frac{\overline{SNR}_E(x, y)}{\overline{SNR}_B + \overline{SNR}_E(x, y)} \end{aligned} \tag{43}$$

where

$$\overline{SNR}_i = \frac{\widetilde{P}_i d_{A,i}^{-b} \mathbb{E}\{|h_{A,i}|^2\}}{N_0 + N_i}$$

with $i = \{B, E\}$ and $\mathbb{E}\{\}$ is the expectation operator.

Thus, the SOPS in this case is

$$A_{out}(\overline{R}_{sec} = 0) = \int_x \int_y \frac{\overline{SNR}_E(x, y)}{\overline{SNR}_B + \overline{SNR}_E(x, y)} \upsilon_E(x, y) dx dy \tag{44}$$

In the case of a target secrecy rate greater than zero $\overline{R}_{sec} > 0$, Eq. (44) is

$$\begin{aligned} &A_{out}(\overline{R}_{sec}) \\ &= \iint_S \text{Prob}\{C_{sec}(x, y) < \overline{R}_{sec}\} \upsilon_E(x, y) dx dy \\ &= \int_x \int_y \left(1 - \frac{\overline{SNR}_B \cdot \exp\left\{ -\frac{2^{\overline{R}_{sec}-1}}{\overline{SNR}_B} \right\}}{\overline{SNR}_B + 2^{\overline{R}_{sec}} \overline{SNR}_E(x, y)} \right) \upsilon_E(x, y) dx dy \end{aligned} \tag{45}$$

The results of the SOPS are shown in Fig. 14. The curves are derived by supposing a Gaussian distribution of the presence of Eve on the surface, i.e.,

$$\upsilon_E(x, y) = \frac{1}{\sqrt{2\sigma_E^2}} e^{\frac{(x - x_E)^2 + (y - y_E)^2}{2\sigma_E}}$$

The other parameters are set as follows: $\mathbb{E}\{|h_{A,i}|^2\} = 1$ with $i = \{B, E\}$, σ_E ranges from 0.2 to 5.

Fig. 14 shows the SOPS ($A_{out}(\overline{R}_{sec} = 0)$) as a function of the standard deviation σ_E of the distribution of Eve's presence on the surface S. Eve is located in three different positions: at Alice's, at Bob's and at the first interferer's I_1. The positions of Alice, Bob and the interferers I_1, I_2 and I_3 are shown in Fig. 4.

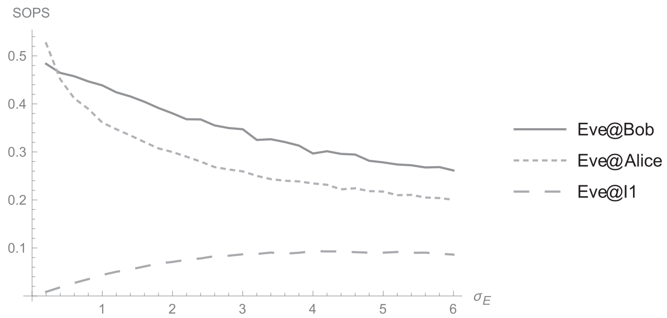


Fig. 14. Secrecy outage of the surface S as a function of the standard deviation σ_E of the distribution of Eve's presence over S. Eve's distribution is Gaussian and centered in three different positions: at Alice's, at Bob's and at the first interferer's I_1.

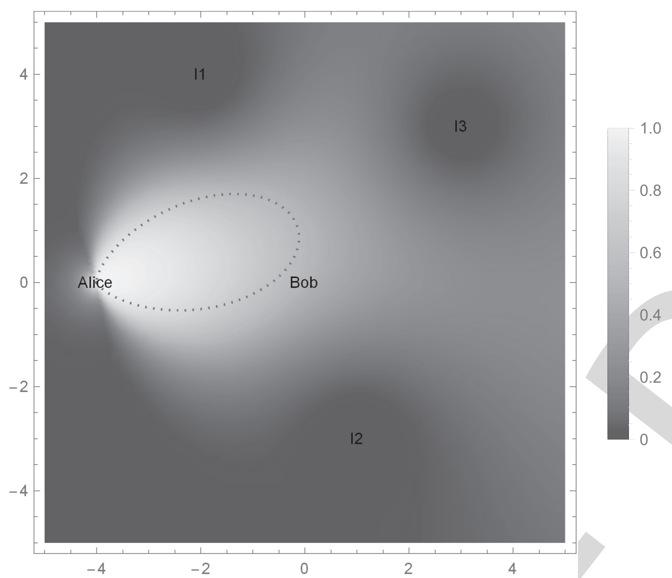


Fig. 15. Secrecy pressure outage map of the surface S.

The orange dotted line in Fig. 14 reports the results when Eve's distribution is centered on the same position of Alice. The curve of the SOPS confirms that a higher dispersion of the probability of Eve's presence yields a lower surface secrecy outage. This is logic, since a higher variance of the Gaussian distribution means higher probability that Eve is located far away from Alice. The green dashed line in Fig. 14 reports the results when Eve's distribution is centered on the same position of the first interferer I_1. The curve of the SOPS, in this case, are completely different from the previous one, as expected. The SOPS increases with the variance σ_E, since a higher dispersion of the position of Eve means a higher probability that Eve is located far away from the interference source, which jams Eve's receiver.

The blue solid line in Fig. 14 reports the results when Eve's distribution is centered on Bob's position. The SOPS increases with the variance σ_E, since a higher dispersion of the position of Eve means a higher probability that Eve is located closer to the source of the information (Alice), i.e., Eve's could have a better signal to noise ratio compared to Bob.

The secrecy pressure outage map of the entire surface is shown in Fig. 15.

VII. Conclusions

This paper proposes and studies a new metric for measuring the secrecy potentials of a surface. This metric is defined secrecy pressure. Using the metric different environments or surfaces can be ordered as a function of the secrecy rate that can be assured. The metric can be used also for solving optimization problems, e.g., finding which is the best transmit antenna orientation to maximize the secrecy capacity of the surface, or finding which is the best position of an additional interfering node (friendly jammer). Different practical scenarios are investigated, including mobility option for the eavesdropper. Another metric, the secrecy outage probability of a surface (SOPS), is derived. In this case the presence of Eve is supposed to be uncertain, and modelled as a Gaussian distribution over the surface. The results of the SOPS are shown as a function of the dispersion of Eve's position. The Gaussian distribution is centered in three specific points: at Alice's, at Bob's and at the first interferer's.

In addition the first part of the paper includes a general framework to evaluate the secrecy capacity over a surface. The framework includes all the parameters affecting the secrecy capacity, from nodes spatial distribution, to antenna orientation and pattern, and propagation medium statistics.

This paper offers a new perspective on the role of secrecy over a surface, considering nodes spatial distribution, wireless propagation medium, and aggregate network interference.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, Aug. 1975, p. 13551387.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Technol. Biomed.*, vol. 24, no. 7, pp. 451–456, Jul. 1978.

[3] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun.*, vol. 6, no. 3, pp. 311–335, Mar. 1998.

[4] Y. Zou, Y.-D. Yao, and B. Zheng, "Opportunistic distributed space-time coding for decode-and-forward cooperation systems," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1766–1781, Apr. 2012.

[5] S. Lakshmanan, C. L. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas, distributed computing systems," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Beijing, China, Jun. 2008, pp. 19–27.

[6] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

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

[8] M. P. Daly, E. Daly, and J. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[9] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 8, pp. 1478–1493, Aug. 2016.

[10] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. 13th Can. Workshop Inf. Theory (CWIT)*, Toronto, ON, Canada, Jun. 2013, pp. 214–218.

[11] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[12] J. M. Carey and D. Grunwald, "Enhancing WLAN security with smart antennas: A physical layer response for information assurance," in *Proc. Veh. Technol. Conf. (VTC Fall)*, Los Angeles, CA, USA, Sep. 2004, pp. 318–320.

[13] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 56–69, Feb. 2015.

[14] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment—Part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.

[15] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[16] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009.

[17] A. Rabbachin, A. Conti, and M. Z. Win, "The role of aggregate interference on intrinsic network secrecy," in *Proc. Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 3548–3553.

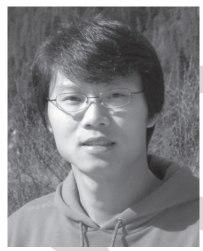
[18] K. I. Pedersen, P. E. Mogensen, and B. H. Fleury, "A stochastic model of the temporal and azimuthal dispersion seen at the base station in outdoor propagation environments," *IEEE Trans. Veh. Technol.*, vol. 49, no. 2, pp. 437–447, Mar. 2000.

[19] H. Asplund, A. A. Glazunov, A. F. Molisch, K. I. Pedersen, and M. Steinbauer, "The COST 259 directional channel model—Part II: Macrocells," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3434–3450, Dec. 2006.

[20] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory'(ISIT)*, Jul. 2006, pp. 356–360.

Lorenzo Mucchi (M'98–SM'12) received the Dr.Eng. (Laurea) degree in telecommunications engineering from the University of Florence, Italy, in 1998, and the Ph.D. degree in telecommunications and information society in 2001. Since 2001, he has been a Research Scientist with the Department of Information Engineering, University of Florence. In 2000, he spent a 12 month period of research at the Center for Wireless Communications, University of Oulu, Finland. He has been a Professor of information technologies with the University of Florence, since 2008. His main research areas include theoretical modeling, algorithm design, and real measurements, mainly focusing on physical-layer security, visible light communications, ultra wideband techniques, localization, adaptive diversity techniques, and interference management. He has authored or co-authored eight book chapters, 32 papers in international journals, and over 80 papers in international conference proceedings during his research activity. He was a member of the IEEE Communications and Information Security Technical Committee in 2009. Since 2016, he has been an Associate Editor of the IEEE COMMUNICATION LETTERS. In 2004, he was the Lead Organizer and the General Chair of the IEEE International Symposium on Medical ICT. He has been the Guest Editor and the Editor-in-chief of the Elsevier Academic Press Library. He was a member of the European Telecommunications Standard Institute Smart Body Area Network (SmartBAN) Group in 2013 and the Team Leader of the special task force 511 SmartBAN Performance and Coexistence Verification in 2016.

Luca Ronga (S'89–M'94–SM'04) received the M.S. degree in electronic engineering and the Ph.D. degree in telecommunications from the University of Florence, Italy, in 1994 and 1998, respectively. In 1997, he joined as a Visiting Scientist the International Computer Science Institute of Berkeley, CA. In 1999, he joined Italian National Consortium for Telecommunications, where he is currently heads the research area. He has authored over 90 papers in international journals and conference proceedings. His research interests span satellite communications to cognitive radio, software-defined radio, radio resource management, and wireless security. He has been an Editor of the *EURASIP Newsletter* for four years, a member of the ETSI SatEC Working Group, and a member of NATO Task Force on Cognitive Radio. He has been a principal investigator in several research projects.



Xiangyun Zhou (M'11) received the Ph.D. degree from The Australian National University (ANU) in 2010. He is currently a Senior Lecturer with ANU. His research interests are in the fields of communication theory and wireless networks. He was a recipient of the Best Paper Award at at ICC in 2011 and the IEEE ComSoc Asia-Pacific Outstanding Paper Award in 2016. He served as a Guest Editor of the *IEEE Communications Magazine* feature topic on wireless physical layer security in 2015. He has also served as the symposium, track, and workshop co-chair for major IEEE conferences. He was the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He currently serves on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE COMMUNICATIONS LETTERS.

Kaibin Huang (M'08–SM'13) received the B.Eng. degree (Hons.) and the M.Eng. degree from the National University of Singapore, and the Ph.D. degree from The University of Texas at Austin (UT Austin), all in electrical engineering. Since 2014, he has been an Assistant Professor with the Department of Electrical and Electronic Engineering (EEE), The University of Hong Kong. He was a Faculty Member with the Department of Applied Mathematics (AMA), The Hong Kong Polytechnic University (PolyU) and the Department of EEE, Yonsei University, South Korea, where he is currently an Adjunct Professor. He is also a University Visiting Scholar with Kansai University, Japan. His research interests focus on the analysis and design of wireless networks using stochastic geometry, and multi-antenna techniques. He received the 2015 IEEE ComSoc Asia Pacific Outstanding Paper Award, the Outstanding Teaching Award from Yonsei, the Motorola Partnerships in Research Grant, the University Continuing Fellowship from UT Austin, and the Best Paper Award from the IEEE GLOBECOM 2006 and PolyU AMA in 2013. He frequently serves on the technical program committees of major IEEE conferences in wireless communications. Most recently, he served as the Lead Chair of the Wireless Communication Symposium of the IEEE Globecom 2017 and the Communication Theory Symposium of the IEEE GLOBECOM 2014 and the TPC Co-Chair of the IEEE PIMRC 2017 and the IEEE CTW 2013. He was an Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Series on Green Communications and Networking from 2015 to 2016, the IEEE WIRELESS COMMUNICATIONS LETTERS from 2011 to 2016, and the IEEE/KICS JOURNAL OF COMMUNICATION AND NETWORKS from 2009 to 2015. He edited the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Special Issue on Communications Powered by Energy Harvesting in 2015. He was an elected member of the SPCOM Technical Committee of the IEEE Signal Processing Society from 2012 to 2015. He is currently an Editor for the newly established IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Yifan Chen (M'06–SM'14) received the B.Eng. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2002 and 2006, respectively. From 2005 to 2007, he was a Project Officer and then a Research Fellow with the Singapore-University of Washington Alliance in bioengineering, supported by the Singapore Agency for Science, Technology and Research, Nanyang Technological University, Singapore, and the University of Washington at Seattle, WA, USA. From 2007 to 2012, he was a Lecturer and then a Senior Lecturer with the University of Greenwich and Newcastle University, U.K. From 2012 to 2016, he was a Professor and the Head of Department of Electrical and Electronic Engineering with the Southern University of Science and Technology, Shenzhen, China, appointed through the Recruitment Program of Global Experts (known as the Thousand Talents Plan). In 2013, he was a Visiting Professor with the Singapore University of Technology and Design, Singapore. He is currently a Professor of Engineering and the Associate Dean External Engagement with the Faculty of Science and Engineering and the Faculty of Computing and Mathematical Sciences, University of Waikato, Hamilton, New Zealand. His current research interests include electromagnetic medical imaging and diagnosis, transient communication with application to healthcare, touchable communication and computation with application to targeted drug delivery and contrast-enhanced medical imaging, fundamentals and applications of nanoscale and molecular communications, and channel modeling for next-generation wireless systems and networks. He is the Coordinator of the European FP7 CoNHealth Project on intelligent medical ICT, an elected Working Group Co-leader of the European COST Action TD1301 MiMed Project on microwave medical imaging, an Advisory Committee Member of the European Horizon 2020 CIRCLE Project on molecular communications, a Voting Member of the IEEE Standards Development Working Group 1906.1 on nanoscale and molecular communications, an Editor for the IEEE ComSoc Best Readings in Nanoscale Communication Networks and the IEEE Access Special Section in Nano-antennas, Nano-transceivers, and Nano-networks/Communications, and a Vice Chair of the IEEE Nano-scale, Molecular and Quantum Networking Emerging Technical Subcommittee.

Rui Wang received the bachelor's degree from the University of Science and Technology of China, in 2004, and the Ph.D. degree in wireless communications from The Hong Kong University of Science and Technology, in 2008. From 2009 to 2012, he was a Senior Research Engineer with Huawei Technologies, Co., Ltd. Since 2012, he has been with the South University of Science and Technology of China, as an Associate Professor. He has research experience in academia and industry. He has authored over 30 papers in top-level IEEE journals and flagship international conferences, especially in the area of wireless radio resource optimization and interference management. He is also involved in the development of interference mitigation technology for 5G systems, and has contributed more than 20 U.S. patent applications and 40 Chinese patent applications (20 of them have been granted).