8-22-2019

Secrecy Capacity and Secure Distance for Diffusion-Based Molecular Communication Systems

Lorenzo Mucchi

Alessio Martinelli

Sara Jayousi

Stefano Caputo

Massimiliano Pierobon

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 21, 2019, accepted July 25, 2019, date of publication August 1, 2019, date of current version August 22, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2932567

Secrecy Capacity and Secure Distance for Diffusion-Based Molecular Communication Systems

LORENZO MUCCHI[1], (Senior Member, IEEE), ALESSIO MARTINELLI[1], SARA JAYOUSI[1], STEFANO CAPUTO[1], AND MASSIMILIANO PIEROBON[2], (Member, IEEE)

[1]Department of Information Engineering, University of Florence, 50139 Florence, Italy
[2]Department of Computer Science and Engineering, University of Nebraska-Lincoln, Lincoln, NE 68508, USA

Corresponding author: Lorenzo Mucchi (lorenzo.mucchi@unifi.it)

This work was supported by the U.S. National Science Foundation under Grant CISE CCF-1816969.

ABSTRACT The biocompatibility and nanoscale features of Molecular Communication (MC) make this paradigm, based on molecules and chemical reactions, an enabler for communication theory applications in the healthcare at its biological level (*e.g.*, bimolecular disease detection/monitoring and intelligent drug delivery). However, the adoption of MC-based innovative solutions into privacy and security-sensitive areas is opening new challenges for this research field. Despite fundamentals of information theory applied to MC have been established in the last decade, research work on security in MC systems is still limited. In contrast to previous literature focused on challenges, and potential roadmaps to secure MC, this paper presents the preliminary elements of a systematic approach to quantifying information security as it propagates through an MC link. In particular, a closed-form mathematical expression for the secrecy capacity of an MC system based on free molecule diffusion is provided. Numerical results highlight the dependence of the secrecy capacity on the average thermodynamic transmit power, the eavesdropper's distance, the transmitted signal bandwidth, and the receiver radius. In addition, the concept of secure distance in an MC system is introduced and investigated for two different techniques of signal detection, *i.e.*, based on energy and amplitude. The secrecy capacity can be used to determine how much secure information (bit/sec/Hz) can be exchanged and within which operative range, while the secure distance can be used to set the transmit power to obtain a secure channel at a given distance. We envision these metrics will be of utmost importance for a future design framework tailored to MC systems and their practical applications.

INDEX TERMS Molecular communication, secrecy capacity, diffusion-based channel, physical-layer security.

I. INTRODUCTION

Molecular Communication (MC) is an interdisciplinary research area between telecommunications, computer science, and biology [1], [2]. The basic idea is that in biological systems, including the human body, the transmitters and receivers communicate by using chemical signals composed of molecules. Telecommunication engineers view MC as a communication paradigm, where the information flows through chemical reactions and molecule transport, as opposed to radio or optical signals. For biologists, MC is an abstraction of how biological cells and their components communicate. During the last decade, researchers devoted more and more efforts in investigating and developing MC-based nano-(bio)-devices and nano-(bio)-networks, and MC is now considered a future (potentially disruptive) communication technology [3]. Communications at molecular level (nanoscale), which make use of chemical reactions and molecule transport processes, have very different rules and objectives compared to the traditional radio communications, whose main objective is to maximize the throughput.

One of the most promising application fields of MC is the healthcare [4], [5], especially in the study of how biological and artificial components (nanosensors, nanoreactors) can

The associate editor coordinating the review of this article and approving it for publication was Daisuke Anzai.

communicate with each other using molecules. The results of these studies will enable a plethora of future applications such as lab-on-a-chip, drug/DNA delivery systems, and human body monitoring using implanted biochemical sensors [3], [6].

More than one decade has been devoted to the study of MC systems, but most of the research has focused on its information theoretical foundations. This research has spanned from the more general and fundamental diffusion-based MC [7], to the more recent application of MC to the tools of synthetic biology [8], [9], where biological cells and their components are studied as programmable computing systems, including the processes at the basis of their interactions.

Secure information transmission has always been an important feature of communication systems, in particular where these systems propagate privacy-sensitive information, such as those related to human health. It is extremely important that security in this new communication paradigm is investigated from the very beginning of its practical development. Adding security features at a later stage, when MC systems are ready to be deployed, could be a serious problem, which could lead to a decrease in the interest for this promising technology.

A. RELATED WORKS

While the aforementioned MC applications are expected to be particularly sensitive to security, security-related issues in MC have been only partially considered. To the knowledge of the authors, the contribution in [10] was the first to address this direction within the broader nanoscale communication field by defining a roadmap for wireless sensor networks security concepts to be reformulated in MC contexts. In particular, the authors introduce the novel notion of biochemical cryptography, where they envision that biological macromolecule composition and structure could be utilized as a medium to maintain information integrity. In [11], the authors shift the attention to security approaches observed in biology, rather than man-made systems, and describe potential directions of research where biochemical cryptography could be based on concepts drawn from the immune system. In [12], two specific attack scenarios focused on MC-enabled target localization operated by programmed biological cells are modeled, as well as countermeasure strategies are proposed and evaluated, where the focus is on the cells' cooperative motility and chemical sensing rather than a single MC channel. Finally, an energy-saving algorithm for secret key exchange between two MC devices based on the Diffie-Hellman method is proposed in [13], without specific security performance considerations.

B. OUR CONTRIBUTION

This paper focuses on the theoretical derivation of the information leakage and secrecy capacity of a diffusion-based MC channel, and a numerical evaluation of the obtained results. As a first step in the aforementioned direction, by stemming from information theoretical results in MC [7], these parameters define how secure a communication link is [14]–[16]. In particular, we provide a closed-form mathematical expression for the secrecy capacity of an MC system based on free molecule diffusion. Numerical results show the secrecy capacity as a function of the distance between transmitter-receiver (Alice-Bob) and transmitter-eavesdropper (Alice-Eve). The MC secrecy capacity is also drawn as a function of the transmitter bandwidth, the average transmit power (thermodynamic power), and the receiver radius, which are important parameters to be considered when designing an MC system.

In addition, the concept of secure distance in a diffusion-based MC system is introduced and investigated for two different techniques of signal detection: energy-based and amplitude-based. This analysis allows us to derive a value for the transmit power that ensures total security at a given distance. Differently from the aforementioned prior literature, the formulas derived in this paper and the numerical results are preliminary elements of a systematic model-based analytical approach to quantifying information security in MC systems.

Part of this paper is based on a previously published conference paper [15]. In particular, we have here performed a deeper analysis of the dependency of the secrecy capacity on different physical-chemical parameters, and we have introduced the concept of secure distance, *i.e.*, the range within which a secure MC can be implemented. The secure distance is analytically derived for both the amplitude-based and the energy-based detection.

C. PRACTICAL MOTIVATION

Molecular communications are nowadays foreseen as a promising method to interface with and coordinate biological systems (including those programmed through synthetic biology), in environments where current technologies have limitations, such as inside the body [5]. For example, programmed cells/organisms can coordinate together to reach a place (tissue) in the body and, when there, activate the production of a molecule, such as an anti-cancer drug. Since the main application is in human health, security is of extreme importance.

Physical-layer Security (PhySec) has recently collected the attention of researchers, since it acts at the physical layer, it is easy to implement, and it provides security without any assumption on the computational power of the attacker. The classical cryptography is based on the assumption that the eavesdropper cannot decipher the message with a "human" amount of time, since it has limited computational power. PhySec, on the contrary, aims at preventing the attacker from demodulating correctly the message, instead of interpreting it. In other words, PhySec makes the demodulation of each single symbol of the message noisy. PhySec could be a good candidate for enhancing the security of biological devices, whose computational power is limited [17].

The analysis reported in this paper is the first investigation on the use of PhySec applied to MC. In particular, we study

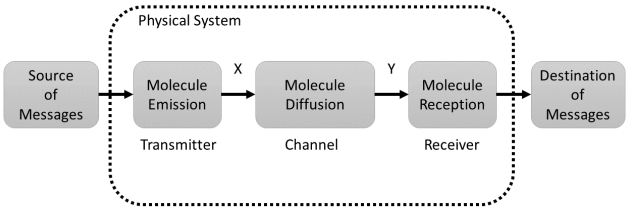


FIGURE 1. The main components of a diffusion-based MC system.

the fundamental benefits and limits of PhySec in diffusion-based channels. Secrecy capacity is derived, which gives us the insight on how many secure symbols a diffusion-based channel can afford. In addition, the paper also explores, more practically, the limit enthalpy (*i.e.*, the "transmit power" in terms of MC) in order to obtain maximum security at a selected distance from the transmitter.

The rest of the paper is organized as follows. Sec. II and Sec. III report a review of the main processes, components, and information-theoretical results at the basis of a diffusion-based MC system, respectively. In Sec. IV, the main contribution of this paper is presented in terms of closed-form expressions for the information leakage and secrecy capacity of such a system. In Sec. V, the concept of secure distance is detailed and mathematically derived. Finally, the obtained numerical results are described in Sec. VI, and concluding remarks are reported in Sec. VII.

II. A DIFFUSION-BASED MOLECULAR COMMUNICATION SYSTEM MODEL

The transmitter, the channel, and the receiver of an MC system are usually abstracted by the processes of molecule emission, diffusion, and reception, respectively, within a physical system, which is the space volume where the communication takes place, as shown in Fig. 1. The physical system is subject to laws and parameters that are affected by how these components are physically realized. The source encodes messages into molecule properties, such as their chemical composition and concentration, before their emission into the space volume, while the destination decodes these messages from the molecule properties sensed by the receiver. Once a message is decoded, the destination reacts according to the meaning and to the particular application. For example, if this communication system is deployed in the human body, as part of an autonomous drug-delivery system, upon reception of a specific concentration of molecules messaging a command, the destination can trigger chemical reactions to synthesize drug molecules.

The physical system considered in this paper is reported in Fig. 2 and it is based on the following assumptions, in agreement with [7]:

- The diffusion-based MC channel extends infinitely in all three dimensions (x, y, z). This space is filled with a fluidic medium having viscosity μ. The fluidic medium does not have flow currents or turbulence, *i.e.*, the propagation is solely due to the Brownian motion;

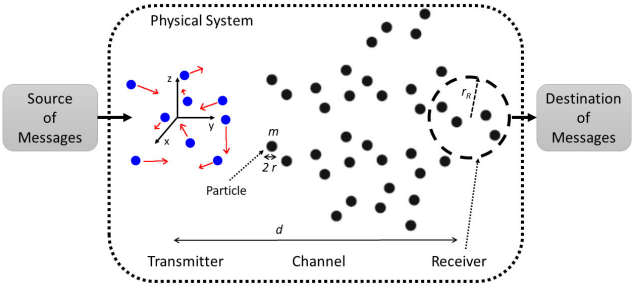


FIGURE 2. Physical realization of a diffusion-based MC system.

- The transmitter emits indistinguishable molecules, equivalent to spherical particles of radius r and mass m;
- The transmitter is considered point-wise and located in $(0, 0, 0)$;
- Each particle, once emitted, moves independently from the others and according to its Brownian motion in the fluid. The Brownian motion of a molecule in a fluid is a random motion according to the Langevin equation [18];
- The (legitimate) receiver detects a signal which is proportional to the concentration of the incoming particles. The receiver location is at a distance d from the transmitter.

As depicted in Fig. 2, the transmitter processes the messages received from the source, and produces a signal suitable for the transmission over the channel. The transmitted signal X is defined as the number of particles $n_{Tx}(t)$ emitted into the fluid as a function of the time t.

The channel propagates the signal from the transmitter to the receiver by means of molecule diffusion, which is the result of the collective translation by Brownian motion of many particles from an area in which they are more dense to an area of lower density. This results in the propagation of the particles emitted by the transmitter throughout the 3D space. This propagation can be expressed as the translation of the 3D coordinates from the location of the transmitter to a location at time t computed by applying the Langevin equation [18] to each particle:

$$m\frac{\partial^2 \mathbf{P}^{[n]}(t)}{\partial t^2} = -6\pi\mu r\frac{\partial \mathbf{P}^{[n]}(t)}{\partial t} + \mathbf{F}(t), \tag{1}$$

where $\mathbf{P}^{[n]} = (P_x^{[n]}, P_y^{[n]}, P_z^{[n]})$ is the position in the 3D space, m is the mass and r is the radius of the particle. μ is the viscosity of the fluid and $\mathbf{F}(t) = (F_x(t), F_y(t), F_z(t))$ is a random process whose probability density function is Gaussian with

$$E\{F_i(t), F_j(t')\} = 12\pi\mu r K_b T\delta(i-j)\delta(t-t'),$$

where K_b is the Boltzmann constant, T is the absolute temperature of the fluid, considered homogeneous throughout the space, and $\delta(.)$ is the Dirac function [19].

The receiver reconstructs the message from the received signal Y, which is proportional to the concentration of incoming particles. We assume here an ideal receiver where the

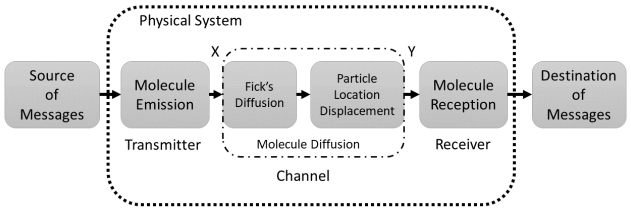


FIGURE 3. The main components of a diffusion-based MC system with the Fick's diffusion and the particle location displacement contributions to the molecule diffusion.

received signal is defined as the time-varying number of particles that are present inside a spherical volume V_R centered at the receiver location and with radius $r_R << d$, where d is the distance between the transmitter and the receiver. This choice makes the results of this paper independent from any specific technique for the reception, such as the use of chemical receptors. As a consequence, the received signal Y is expressed as the number of particles emitted by the transmitter from time instant 0 to time instant t whose location $\mathbf{P}^{[n]}(t)$ is inside the volume V_R.

III. INFORMATION CAPACITY OF A DIFFUSION-BASED MOLECULAR COMMUNICATION SYSTEM

The information capacity of a communication system is expressed by the general formula from Shannon [16]. The general equation defines the information capacity as the maximum difference between the entropy $H(X)$ of the signal X input of the channel and the equivocation $H(X|Y)$, which represents the entropy of X conditioned to the observation signal Y at the destination, as follows:

$$C = \max_{f_X(x)} I(X;Y) = \max_{f_X(x)} \{H(X) - H(X|Y)\}. \tag{2}$$

From the physical system defined in Sec. II, two phenomena play an important role in the quantification of the mutual information $I(X;Y)$: the channel memory and the molecular noise. In [7] the computation of the mutual information is divided into two processes: the Fick's diffusion, which captures solely the effects of the channel memory, and the particle location displacement, which isolates the effects of the molecular noise (Fig. 3).

The expression of the mutual information of a diffusion-based MC system is analytically derived in [7] as

$$\begin{aligned} I(x;y) = {} & 2WH(\overline{n}_{Tx}) - \log_2\left[(\pi dD)^2\right] - \frac{4d}{3\ln 2}\sqrt{\frac{\pi W}{D}} \\ & - 2W\eta - 2W\ln(W\tau_p) - 2W\ln(\Gamma(\eta)) \\ & - 2W(1-\eta)\psi(\eta), \end{aligned} \tag{3}$$

where

$$\begin{aligned} \eta &= \frac{2E[\overline{n}_{Tx}]R_{V_R}}{3\,Wd}, \\ E[\overline{n}_{Tx}] &= \frac{\overline{P}_H}{3WK_bT}, \\ H(\overline{n}_{Tx}) &= 1 + \log_2\, E[\overline{n}_{Tx}], \end{aligned}$$

and

- W is the bandwidth of the transmitted signal X, intended as the set of frequency components contained in the Fourier transform of the signal;
- $\tau_p = \frac{r_R^2}{D}$ is the time interval in which we consider a quasi-constant particle distribution, which depends on how fast on average particles can escape the receiver volume;
- $\Gamma(.)$ is the gamma function and $\psi(.)$ is the digamma function;
- $D = \frac{K_bT}{6\pi\mu r}$ is the diffusion coefficient, which depends on the molecule and physical environment parameters defined above;
- d is the distance between the transmitter and the receiver;
- r_R is the radius of the spherical receiver volume;
- $\overline{P}_H$ is the average thermodynamic power, which corresponds to the energy necessary to emit $E[\overline{n}_{Tx}]$ particles per time interval τ_p in the physical system and to heat these particles up to a temperature T when the system has the pressure P and the volume V;
- $\overline{n}_{Tx}$ is the discrete-time version of the particle concentration $n_{Tx}(t)$.

From (2) and (3) the expression of the capacity C of the diffusion-based MC system [7] is obtained as

$$\begin{aligned} C = {} & 2W\left(1 + \log_2 \frac{\overline{P}_H}{3WK_bT}\right) - \log_2\left[(\pi dD)^2\right] \\ & - \frac{4d}{3\ln 2}\sqrt{\frac{\pi W}{D}} - 2W\eta - 2W\ln\left(W\frac{r_R^2}{D}\right) \\ & - 2W\ln(\Gamma(\eta)) - 2W(1-\eta)\psi(\eta). \end{aligned} \tag{4}$$

The parameters in (4) are defined above as for (3).

IV. INFORMATION LEAKAGE AND SECRECY CAPACITY

The information-theoretical security computes exactly the amount of information that an eavesdropper (Eve) can get by observing the channel, while the legitimate communication is ongoing. The generic reference scheme for evaluating the information-theoretical security of an MC system is reported in Fig. 4. Alice is the cell that transmits the particles, Bob is the intended legitimate receiver, and Eve is the eavesdropping receiver.

The amount of information that is exchanged by Alice and Bob is given by (3), while the amount of information "stolen" by Eve is called information leakage. In information-theoretical security, the information leakage can be written as [14]

$$I(X;Z) = H(X) - H(X|Z), \tag{5}$$

where Z is the signal observed by Eve. The eavesdropper receiving particles is supposed to be at distance d_E from the transmitter. The secrecy capacity of the diffusion-based channel can be derived as the maximum of the difference between the mutual information of the legitimate communication link and the information leakage [14]. It is important to note that

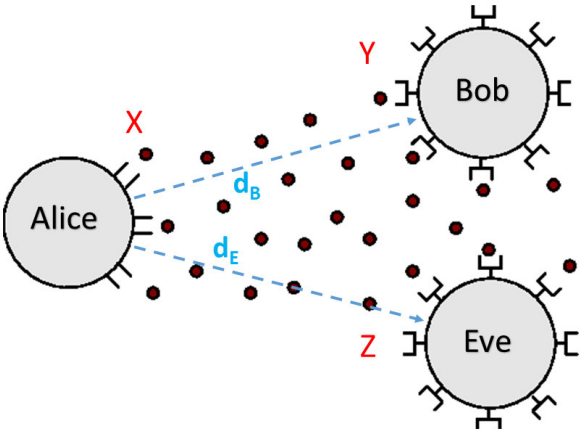


FIGURE 4. Scheme for the evaluation of the information-theoretical security of a diffusion-based MC system.

the definition of secrecy capacity has to be intended as an upper bound of the security performance of a communication system. The following inequality can then be derived:

$$C_s = \max_{f_X(x)} \{I(X;Y) - I(X;Z)\}$$
$$\geq \max\{I(X;Y)\} - \max\{I(X;Z)\} = C_B - C_E, \quad (6)$$

where C_B is the capacity of the legitimate channel and C_E is the capacity of Eve's channel, and the last formula expresses a lower-bound estimation of the secrecy capacity that can be derived from the aforementioned MC capacity formula. Since the secrecy capacity cannot be less than zero, (6) is usually written as

$$C_s = \max\{0, C_B - C_E\}. \quad (7)$$

Both C_B and C_E can be computed by using (4). The secrecy capacity in (7) represents the amount of information that can be securely exchanged between two legitimate MC components (transmitter and receiver), while an eavesdropping component is "overhearing" the diffusion-based channel, which exhibits a broadcasting nature.

The capacity of the legitimate receiver (Bob) is

$$C_B = 2W\left(1 + \log_2 \frac{\overline{P}_H}{3WK_bT}\right) - \log_2\left[(\pi d_B D)^2\right]$$
$$- \frac{4d_B}{3\ln 2}\sqrt{\frac{\pi W}{D}} - 2W\eta_B - 2W\ln\left(W\frac{r_{R_B}^2}{D}\right)$$
$$- 2W\ln(\Gamma(\eta_B)) - 2W(1-\eta_B)\psi(\eta_B), \quad (8)$$

where

$$\eta_B = \frac{2\overline{P}_H r_{R_B}}{9W^2K_bTd_B}. \quad (9)$$

The capacity of Eve's receiver can be computed by substituting d_B and r_{R_B} with d_E and r_{R_E}, respectively, into (8) and (9).

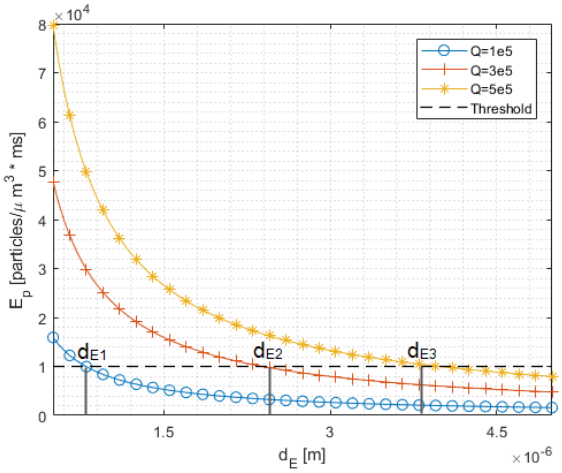


FIGURE 5. Signal energy E_P as a function of the eavesdropper's distance d_E for several values of transmitted particles Q. The signal energy threshold $\bar{E}$ is set to 10^4 particles/μm^3 · *m*sec.

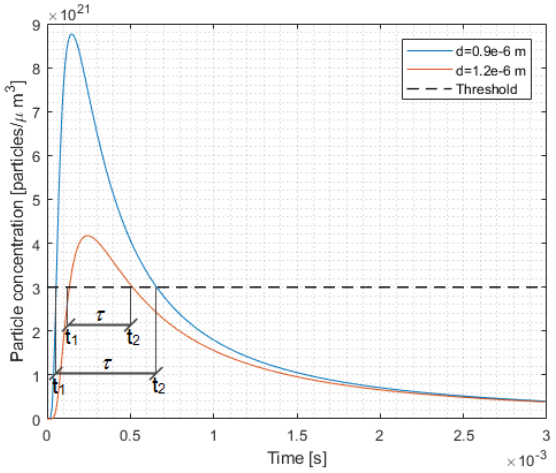


FIGURE 6. Particle concentration as a function of the distance between transmitter and receiver. The concentration threshold leads to the identification of a time interval $\tau = t_2 - t_1$, which decreases with increasing distance.

The secrecy capacity of a MC diffusion-based system is

$$C_s = \log_2\left[\left(\frac{d_E}{d_B}\right)^2\right] + \frac{4}{3\ln 2}\sqrt{\frac{\pi W}{D}}(d_E - d_B)$$
$$+ 2W(\eta_E - \eta_B) + 2W\ln\left[\left(\frac{r_{R_E}}{r_{R_B}}\right)^2\right] + 2W\ln\left[\frac{\Gamma(\eta_E)}{\Gamma(\eta_B)}\right]$$
$$+ 2W\left[(1-\eta_E)\,\psi(\eta_E) - (1-\eta_B)\,\psi(\eta_B)\right]. \quad (10)$$

V. SECURE DISTANCE IN A MOLECULAR COMMUNICATION SYSTEM

In the scenario depicted in Fig. 4, the reliability and the secrecy of the communication link between the transmitter (Bob) and the legitimate receiver (Alice) rely on the fulfillment of the following two conditions, respectively: 1) the

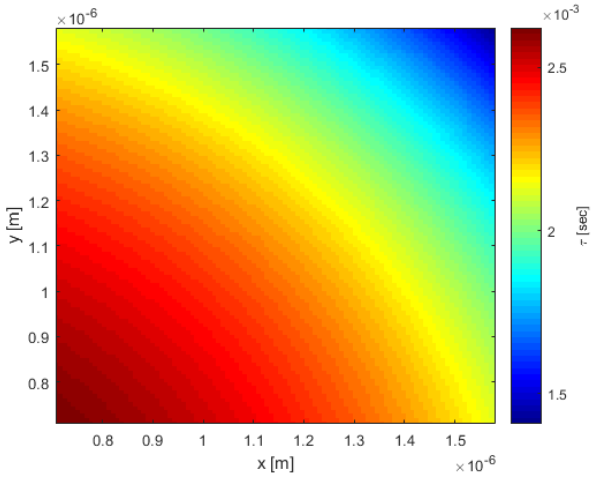


FIGURE 7. 2D map of τ. The number of transmitted particles is $Q = 10^3$. The threshold of particle concentration $\bar{c}$ is 50 particles/μm^3.

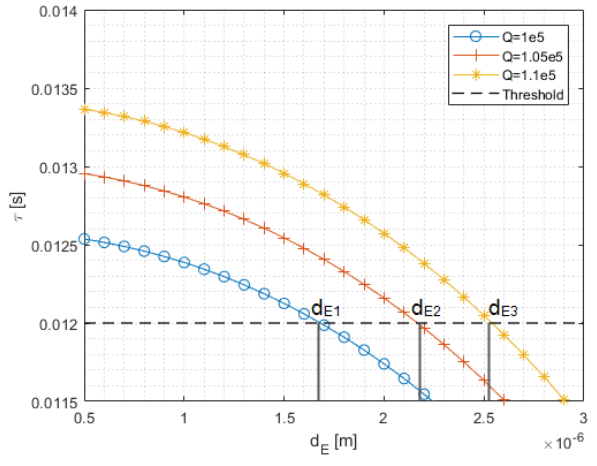


FIGURE 8. τ as a function of the eavesdropper's distance d_E for several values of transmitted particles Q. The threshold $\bar{\tau}$ is set to 0.012 seconds.

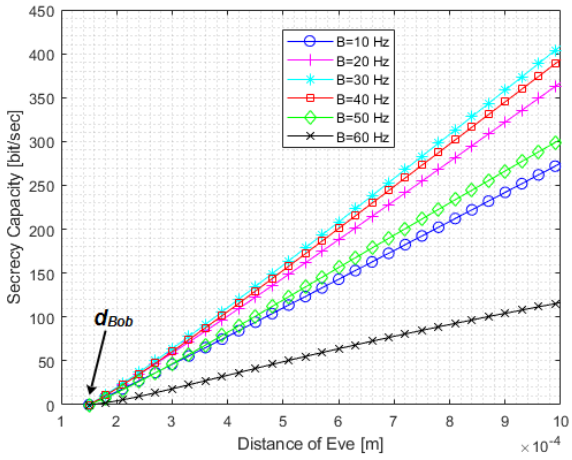


FIGURE 9. Secrecy capacity as a function of the distance of the eavesdropper, for several values of the transmitted signal bandwidth. The distance of the legitimate receiver (Bob) is 150 μm.

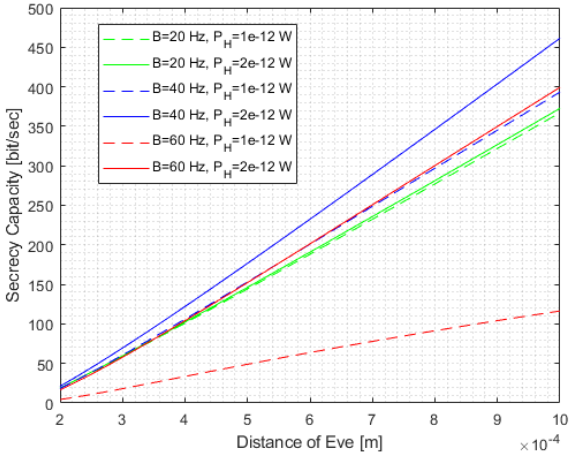


FIGURE 10. Secrecy capacity as a function of the distance of the eavesdropper, for several values of the transmitted signal bandwidth and power. The distance of the legitimate receiver (Bob) is 150 μm.

legitimate receiver correctly detects the information signal (reliability); 2) the eavesdropper (Eve) is not able to detect the information signal (security). In a communication system, the characteristics of reliability and secrecy depend on the receiver type. In particular, in a diffusion-based MC system, the receivers generally rely on two detection techniques, namely, energy detection and amplitude detection [2].

By solving the Fick's law of diffusion [7], the particle concentration at distance d and time t is obtained as follows:

$$c(d,t) = \frac{Q}{(4\pi Dt)^{3/2}} e^{\frac{-d^2}{4Dt}} \tag{11}$$

where D is the diffusion coefficient, Q is the number of molecules emitted, and d is the distance from the transmitter.

A. ENERGY DETECTION

Let us now suppose that the receiver acts like an energy detector [20]. The receiver decides that an information signal is detected if the amount of particles (signal energy) received over time is greater than a given threshold. In the following, the molecular signal energy is defined as a function of d:

$$E_p(d) = \int_0^\infty c(d,t)dt = \int_0^\infty \frac{Qe^{\frac{-d^2}{4Dt}}}{(4\pi Dt)^{3/2}} dt = \frac{Q}{4\pi Dd}. \tag{12}$$

The secrecy of the communication link between the transmitter and the legitimate receiver is guaranteed if the amount of particles accumulated over time (signal energy) by the eavesdropper is below a threshold $\bar{c}$, which corresponds to the receiver sensitivity, thus the eavesdropper is not able to detect the signal. A secure communication channel can be defined by identifying the number of transmitted particles $\overline{Q}$ so that the pulse energy measured above the distance d_E is less than or equal to the threshold $\overline{E}$, expressed as

$$\overline{Q} : E_p(d) \le \overline{E}, \quad \forall d \ge d_E. \tag{13}$$

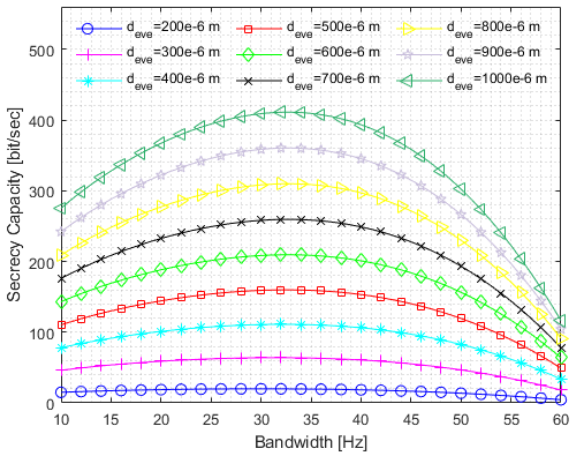


FIGURE 11. Secrecy capacity as a function of the transmitted signal bandwidth, for several values of the eavesdropper's distance. The distance of the legitimate receiver (Bob) is 150 μm.

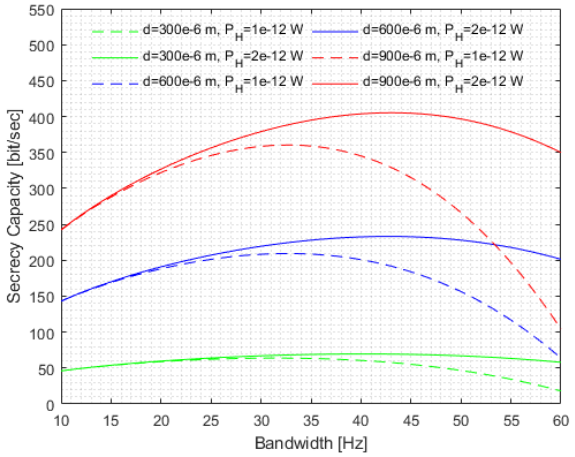


FIGURE 12. Secrecy capacity as a function of the transmitted signal bandwidth, for several values of the eavesdropper's distance and transmit power. The distance of the legitimate receiver (Bob) is 150 μm.

Using (12) to solve (13), we obtain

$$\overline{Q} \leq \overline{E} 4\pi D d_E.$$

Based on this scheme, the transmit power that prevents the eavesdropper to detect the information signal can be derived. Fig. 5 shows the dependency of the signal energy E_p on the distance d_E (Eve's receiver - transmitter distance) for different values of the number of transmitted particles Q. Given the number of transmitted particles, we can find the distance above which a total security of the communication can be guaranteed. Considering the graphs reported in Fig. 5, if the number of transmitted particles is set to $Q = 1e5$, then d_{E1} represents the distance limit above which a potential eavesdropper is not able to detect the transmitted information.

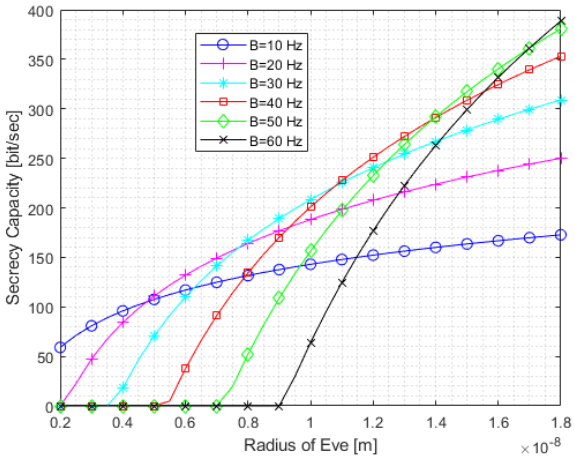


FIGURE 13. Secrecy capacity as a function of the eavesdropper's radius, for several values of the transmitted signal bandwidth. The distance of the legitimate receiver (Bob) and the eavesdropper (Eve) is 150 μm. The radius of Bob is 10 nm.

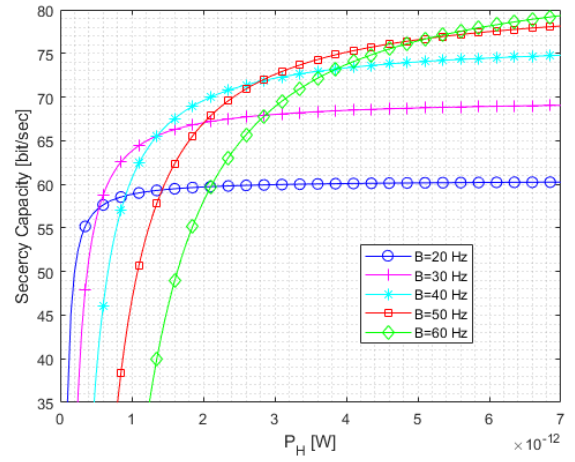


FIGURE 14. Secrecy capacity as a function of the transmit power, for several values of the transmitted signal bandwidth. The distance of the legitimate receiver (Bob) is 150 μm.

B. AMPLITUDE DETECTION

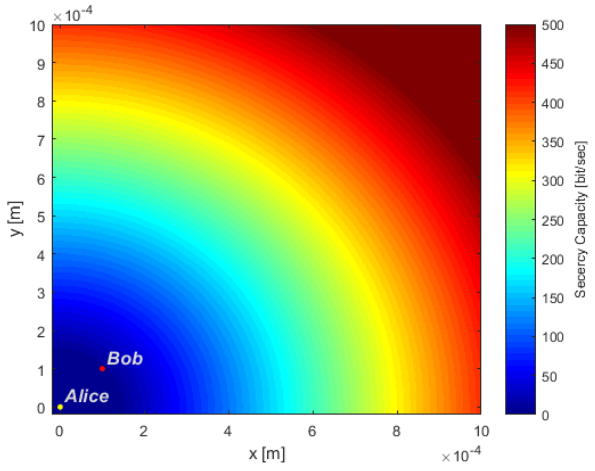
We assume that the receiver decides that an information signal is received based on the measured concentration of molecules. In particular, the receiver detects an information signal if the concentration stays over a threshold for a given time interval (amplitude detector). In order to find the time values so that the concentration at a distance d_R is greater than a threshold $\overline{c}$, we solve the following equation:

$$\frac{Q}{(4\pi Dt)^{3/2}} e^{\frac{-d_R^2}{4Dt}} = \overline{c}, \tag{14}$$

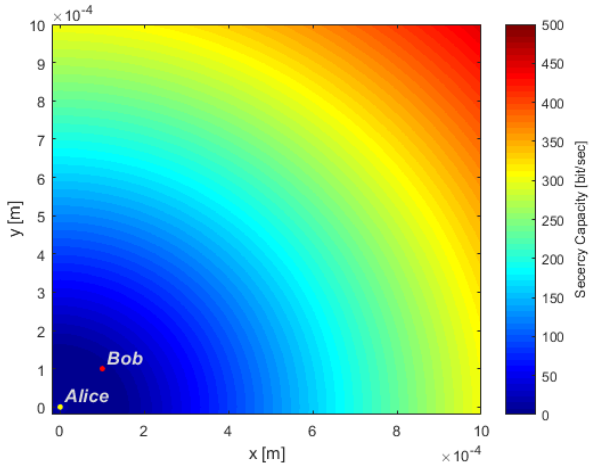
which gives

$$t = -\frac{d_R^2}{f_W\left(-\frac{2}{3}\pi d_R^2 (\frac{\overline{c}}{Q})^{\frac{2}{3}}, \right) 6D} \tag{15}$$

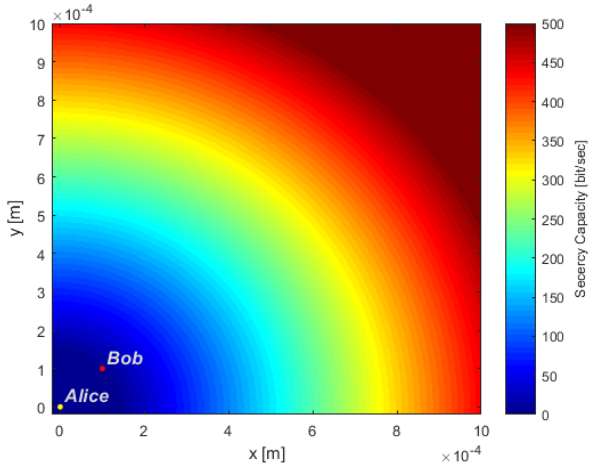
where $f_W(\cdot)$ is the Lambert W-function [21]. The two solutions of (15) are named t_1 and t_2 and the difference $t_2 - t_1 = \tau$



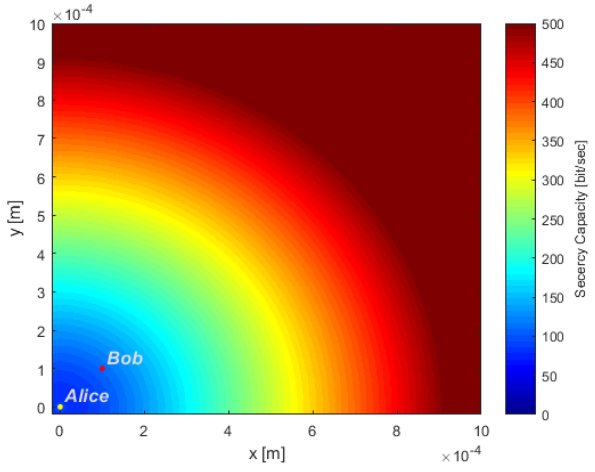
(a) Secrecy map when $B = 30$ Hz, $\overline{P}_H = 1 \cdot 10^{-12}$ W, $r_{R_B} = r_{R_E} = 10 \cdot 10^{-9}$ m.



(b) Secrecy map when $B = 50$ Hz, $\overline{P}_H = 1 \cdot 10^{-12}$ W, $r_{R_B} = r_{R_E} = 10 \cdot 10^{-9}$ m.



(c) Secrecy map when $B = 30$ Hz, $\overline{P}_H = 2 \cdot 10^{-12}$ W, $r_{R_B} = r_{R_E} = 10 \cdot 10^{-9}$ m.



(d) Secrecy map when $B = 30$ Hz, $\overline{P}_H = 1 \cdot 10^{-12}$ W, $r_{R_B} = 10 \cdot 10^{-9}$ m, $r_{R_E} = 20 \cdot 10^{-9}$ m.

FIGURE 15. 2D map of the secrecy capacity. The transmitter (Alice) is positioned in (0, 0), while the legitimate receiver (Bob) is located in (100, 100) μm.

represents the time interval in which the concentration of the particles remains above the threshold $\overline{c}$.

Fig. 6 shows how the time interval τ is determined for different distances by selecting a threshold of particle concentration. Fig. 7 shows the 2D map of τ when $Q = 10^3$ and the threshold is set to 50 particles/μm^3. It is evident that τ fades when the distance increases.

Given a threshold $\overline{\tau}$ for which the receiver detects the information signal (receiver's sensitivity), we can derive from (15) a suitable value for the distance so that $\overline{\tau}$ is not reached, and the security is preserved. Figs. 8 illustrates the variation of τ against the eavesdropper's distance for different number of transmitted particles: the threshold $\overline{\tau}$ set to 0.012 seconds leads to the identification of a secure distance d_E for each transmit power. Given the threshold $\overline{\tau}$, the number of transmitted particles that may guarantee a secure communication over a certain distance can be identified.

VI. NUMERICAL RESULTS

In this section, we provide a numerical evaluation of the closed-form expression for the previously described diffusion-based MC secrecy capacity. All results are computed for a common set of parameters, whose values are assigned as follows:

- the radius of the receiver volume, assumed to be spherical, is $r_{R_B} = r_{R_E} = 10 \cdot 10^{-9}$ m [22];
- the temperature of the system is set to a standard room temperature $T = 298.15$ °K;
- the diffusion coefficient is set to $D = 10^{-9}$ m^2/s [22];
- the Boltzmann constant is equal to $K_b = 1.380650424 \cdot 10^{-23}$ J/K.

Fig. 9 shows the secrecy capacity as a function of Eve's distance for different values of the bandwidth of the transmitted signal. The distance of the legitimate receiver is 150μm. While the distance of Eve is lower than the distance of Bob,

C_s is zero. As the distance of Eve increases, the secrecy capacity grows. The slope of C_s is lower for high values of the bandwidth.

Fig. 10 reports the secrecy capacity as a function of the distance of Eve, for several values of the transmitted signal bandwidth and transmit power. In particular, the transmit power can assume values 1 or 2 pW. Doubling the transmit power at the same bandwidth yields a lower C_s, and this effect is more evident for larger values of the transmitted signal bandwidth.

Fig. 11 shows the secrecy capacity as a function of the bandwidth, for different distances of Eve. The distance of the legitimate receiver is 150 μm. While the distance of Eve is lower than the distance of Bob, the C_s is zero for any value of bandwidth. As the distance of Eve increases, the C_s increases up to $B = 30$ Hz and then it starts decreasing. For high bandwidth $B = 60$ Hz, a greater distance of Eve does not yield a much larger secrecy capacity.

Fig. 12 shows the secrecy capacity as a function of the bandwidth, for different distances of Eve and transmit power. In particular, doubling the transmit power improves C_s for a transmitted signal bandwidth larger than 20 Hz, and this effect is more evident for higher distances of the eavesdropper.

Fig. 13 shows the secrecy capacity as a function of Eve's radius, for several values of the transmitted signal bandwidth. Bob and Eve distance is 150 μm, and Bob's radius is 10 nm. A higher bandwidth (60 Hz) yields a $C_s = 0$ since the radius of Eve is almost equal to Bob's (0.9 nm). This effect fades if the transmitted signal bandwidth decreases. For $B = 10$ Hz we obtain $C_s > 0$ for every value of Eve's radius, although the secrecy capacity reaches a lower value.

Fig. 14 shows C_s as a function of the transmit power P_H, for several values of the transmitted signal bandwidth. Increasing the power seems to saturate C_s. The lower the bandwidth, the lower the saturation value.

The range of the bandwidth has been limited to $B \in [20, 60]$ Hz, since according to [23], the neurons of human brain communicate through the diffusion of molecules between the synapses (a natural diffusion-based MC system) at a frequency of 20 Hz for the processing of general information and 60 Hz for visual images.

Fig. 15 shows the 2D map of the secrecy capacity. The secrecy map is calculated by assuming that Eve is located in a generic point (x, y) of the surface and computing the C_s [24]. The transmitter (Alice) is positioned in (0, 0), while the legitimate receiver (Bob) is located in (100, 100) μm. For the sake of clarity, we decided to show only the first quadrant, but the C_s is spherical. In other words, the expression of the secrecy capacity considers (and it is valid for) a 3D spherical system; the 2D representation has been selected only for easier display of the results. The four secrecy maps in Fig. 15 have been selected to highlight the dependency of the C_s on the transmitted signal bandwidth, the transmit power, and the receiver radius.

Analyzing Figs. 15a and 15b, we can appreciate the effect of doubling the bandwidth. As expected, a greater bandwidth at the transmitter results into a larger portion of space where the secrecy capacity is zero. In general, doubling the bandwidth makes the "strips" of the secrecy map larger.

The same effect is provided if the transmit power is increased. In fact, by observing Figs. 15a and 15c we can conclude that increasing $\overline{P}_H$ yields larger "strips" in the secrecy capacity map. In other words, a higher transmit power produces lower secrecy capacity, since Eve can be located in more points of the surface where it can receive information.

Observing Figs. 15a and 15d we can appreciate the effect of doubling the radius of Bob's receiver. This produces a drastic decrease of the C_s, since the lingand-receptor binding noise increases with the receiver's radius [25]. The ligand-receptor binding noise is a model which allows to simulate the random perturbations in the chemical processes of the reception.

VII. CONCLUSION

In this paper, we provided closed-form mathematical expressions for the information leakage and secrecy capacity of an MC system. These metrics are useful to define the security of a communication link where information is propagated by molecule diffusion. The secrecy capacity is a function of the medium diffusion coefficient, the system temperature, and, in particular, the distance between the MC transmitter and receiver (Alice-Bob) and the MC transmitter and a potential eavesdropper (Alice-Eve). The MC secrecy capacity is also function of the bandwidth, average thermodynamic transmit power, and receiver radius. Numerical results presented in this paper show the dependencies of the MC secrecy capacity with respect to all these parameters. Moreover, a secrecy map has been drawn to graphically show where the secure-insecure areas are located in the space adjacent to the MC system.

According to the obtained results, a secrecy rate of 60 bit/sec can be reached if Eve's distance is twice the distance of the legitimate transmitter-receiver, for an average thermodynamic transmit power of 1 pW and a bandwidth of 20 Hz. The numerical results have to be intended as an upper bound to the security performance of a diffusion-based MC system.

In addition, depending on the detection mechanism of the receiver (amplitude or energy detector), the transmit power to get full security at a given distance has been analytically derived. This result could be used to design transmitting and corresponding receiving MC devices that realize secure communications in a biochemical environment at a given range of operation.

We envision that the metrics derived in this paper (secrecy capacity and secure distance) will be of utmost importance for developing future technologies based on MC systems and their practical applications.

REFERENCES

[1] I. F. Akyildiz, J. M. Jornet, and M. Pierobon, "Nanonetworks: A new frontier in communications," *Commun. ACM*, vol. 54, no. 11, pp. 84–89, Nov. 2011. doi: 10.1145/2018396.2018417.
[2] T. Nakano, "Molecular communication: A 10 year retrospective," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 3, no. 2, pp. 71–78, Jun. 2017.
[3] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The Internet of bio-nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015.
[4] Y. Moritani, S. Hiyama, and T. Suda, "Molecular communication for health care applications," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOMW)*, Mar. 2006, p. 5 and 553.
[5] I. F. Akyildiz, M. Pierobon, and S. Balasubramaniam, "Moving forward with molecular communication: From theory to human health applications [point of view]," *Proc. IEEE*, vol. 107, no. 5, pp. 858–865, May 2019.
[6] R. E. Oosterbroek and A. van den Berg, *Lab-on-a-Chip: Miniaturized Systems for (Bio)Chemical Analysis and Synthesis*. Amsterdam, The Netherlands: Elsevier, 2003.
[7] M. Pierobon and I. F. Akyildiz, "Capacity of a diffusion-based molecular communication system with channel memory and molecular noise," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 942–954, Feb. 2013.
[8] A. Marcone, M. Pierobon, and M. Magarini, "Parity-check coding based on genetic circuits for engineered molecular communication between biological cells," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6221–6236, Dec. 2018.
[9] C. Harper, M. Pierobon, and M. Magarini, "Estimating information exchange performance of engineered cell-to-cell molecular communications: A computational approach," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2018, pp. 729–737.
[10] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Commun. Netw.*, vol. 3, no. 3, pp. 151–160, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1878778912000294
[11] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 198–207, Sep. 2014.
[12] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 665–676, Apr. 2016.
[13] S. M. R. Islam, F. Ali, H. Moon, and K.-S. Kwak, "Secure channel for molecular communications," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2017, pp. 1–4.
[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[15] L. Mucchi, A. Martinelli, S. Caputo, S. Jayousi, and M. Pierobon, "Secrecy capacity of diffusion-based molecular communication systems," in *Proc. 13th EAI Int. Conf. Body Area Netw. (BodyNets)*, Oct. 2018, pp. 1–5.
[16] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley Series in Telecommunications and Signal Processing). New York, NY, USA: Wiley, 2006.
[17] R. Sarpeshkar, "Analog synthetic biology," *Philos. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 372, no. 2012, pp. 1–22, 2014.
[18] D. S. Lemons, "Paul Langevin's 1908 paper 'On the theory of Brownian motion' ['Sur la théorie du mouvement brownien,' C. R. Acad. Sci. (Paris) 146, 530–533 (1908)]," *Amer. J. Phys.*, vol. 65, no. 11, pp. 1079–1081, Nov. 1997.
[19] S. Hassani, *Mathematical Methods: For Students of Physics and Related Fields*. New York, NY, USA: Springer-Verlag, 2009.
[20] I. Llatser, A. Cabellos-Aparicio, M. Pierobon, and E. Alarcon, "Detection techniques for diffusion-based molecular communication," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 12, pp. 726–734, Dec. 2013.
[21] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the LambertW function," *Adv. Comput. Math.*, vol. 5, pp. 329–359, Dec. 1996. doi: 10.1007/BF02124750.
[22] M. Pierobon and I. F. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 4, pp. 602–611, May 2010.
[23] D. L. Nelson and M. M. Cox, *Lehninger Principles of Biochemistry*. San Francisco, CA, USA: Freeman, 2005.
[24] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3416–3430, May 2017.
[25] M. Pierobon and I. F. Akyildiz, "Noise analysis in ligand-binding reception for molecular communication in nanonetworks," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4168–4182, Sep. 2011.

LORENZO MUCCHI (M'98–SM'12) received the Laurea degree in telecommunications engineering and the Ph.D. degree in telecommunications and information society from the University of Florence, Italy, in 1998 and 2001, respectively. He is currently an Associate Professor with the University of Florence, Italy. His research interests involve theory and experimentation of wireless systems and networks, including physical-layer security, visible light communications, ultra-wideband techniques, body area networks, and interference management. He is currently serving as an Associate Editor for the IEEE COMMUNICATIONS LETTER and IEEE ACCESS, and he has been the Editor-in-Chief for the *Elsevier Academic Press*. He is a member of the European Telecommunications Standard Institute (ETSI) Smart Body Area Network (SmartBAN) Group (2013) and the Team Leader of the Special Task Force 511 (2016) 'SmartBAN Performance and Coexistence Verification'. He has been the lead organizer and the General Chair of the IEEE and EAI international conferences.

ALESSIO MARTINELLI received the Ph.D. degree in information engineering from the University of Florence, in April 2017, where he is currently a Research Fellow with the Department of Information Engineering. His research activity is mainly focused on positioning and navigation solutions: ultra-wide band positioning, cooperative GNSS positioning, GNSS/INS integration techniques, and pedestrian dead Reckoning navigation.

SARA JAYOUSI received the M.S. degree in telecommunications engineering, and the Ph.D. degree in computer science, multimedia and telecommunications from the University of Florence, Italy, in 2008 and 2012, respectively. She has been with the Department of Information Engineering, University of Florence, since 2008, under research contracts on satellite/terrestrial communication networks topics. Her research activity is mainly focused on satellite communications for emergency, IP QoS network management in hybrid satellite/terrestrial networks, cooperative communications, and diversity algorithms in relaying systems. She has been involved in national and European research projects (ESA projects) on heterogeneous wireless communication systems for e-Health and Emergency service provision. She was a member of the ETSI Specialist Task Force 473 for the standardization of multiple alert message encapsulation protocol for transporting alert messages over satellite links. Her research activity is testified by papers published in international journals and conferences.

STEFANO CAPUTO was born in Florence, Italy, in 1984. He received the Dr. Eng. degree (Laurea) in mechanical engineering from the University of Florence, Italy, in 2016, where he is currently pursuing the Ph.D. degree in telecommunications engineering. From 2010 to 2011, he spent an 18-month period of work as Mechanical Engineer for designing CNC Machine. His main research areas include theoretical modeling, algorithm design, and real measurements, mainly focused in the following fields, such as the physical-layer security and light cryptography, sensors and V2V/V2I communication in automotive field, visible light communications, localization, body area networks, and molecular communications.

MASSIMILIANO PIEROBON (S'09–M'13) received the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2013. Since August 2013, he has been an Assistant Professor with the Department of Computer Science and Engineering, University of Nebraska-Lincoln (UNL), NE, USA, where he also holds a courtesy appointment at the Department of Biochemistry. He is the Co-Editor-in-Chief of the *Nano Communication Networks* (Elsevier), since July 2017, and an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, since 2013. His selected honors include 2017 IEEE INFOCOM Best Paper Runner-up Award, and the IEEE GLOBECOM 2017 Best Paper Award. He is currently the PI of multiple NSF projects in the field of molecular communication applied to biological systems. His research interests are in molecular communication theory, nanonetworks, intra-body networks, communication engineering applied to synthetic biology, and the Internet of Bio-Nano Things. He is a faculty mentor for the UNL iGEM team, since 2016.