Secrecy Optimization for Diffusion-Based Molecular Timing Channels

Gaurav Sharma, *Graduate Student Member, IEEE*, Nilay Pandey, *Member, IEEE*, Ajay Singh, *Member, IEEE*, and Ranjan K. Mallik, *Fellow, IEEE*

***Abstract*—Security in the context of molecular communication systems is an important design aspect that has not attracted much attention till date. This letter analyzes the information-theoretic secrecy of diffusive molecular timing channels when the distance of the eavesdropper is assumed to be random and uniformly distributed. Using an existing upper bound on the timing channel capacity, we calculate the optimal secrecy rate and optimal transmission rate for Bob which would help in achieving an improved secrecy throughput performance. Based on this optimal rate, we calculate the maximum achievable throughput. We then use this formulation to minimize the generalized secrecy outage probability (GSOP) by simultaneously maximizing the average fractional equivocation and minimizing the average information leakage rate. The numerical results show that while choosing the system parameters, there is always a trade-off between different performance metrics like GSOP, average fractional equivocation, and average information leakage rate. The proposed secrecy optimization provides a robust understanding of the physical layer secrecy at the molecular level, enabling the design of secure molecular communication systems.**

***Index Terms*—Average fractional equivocation, average information leakage rate, generalized secrecy outage probability, information-theoretic secrecy, molecular timing channel.**

I. Introduction

TRADITIONAL communication engineering research has mostly focused on the transmission of information from the transmitter to the receiver using electromagnetic (EM) waves travelling over wired, wireless, or optical media. However, with the advancements in the field of nanotechnology, it is now possible to develop and deploy nano and microscale devices that need to transmit and receive information at the microscopic level. At such small scales, the conventional means of communication using EM waves fail to deliver promising results. For such microscale environments, molecular communication (MC) where information is exchanged chemically by exchanging information molecules has emerged as a promising communication option [1], [2], [3]. Though MC research from an engineering perspective is relatively new, this kind of communication involving molecules such as pollen, pheromones, hormones, etc., is very prominent in natural and biological systems [4], [5].

Transmission of the information is achieved by modulating certain characteristics of these information molecules. Some of these characteristics include time of release [3], concentration [2], number [6], position [7], or type [8]. Furthermore, the transportation of the information molecules can be achieved via pure diffusion, flow assisted diffusion, molecular motors, and engineered bacteria [2]. In a diffusion-based MC channel, the channel is usually some kind of aqueous medium connecting the transmitter to the receiver. An information molecule released in such a medium propagates through the underlying process of Brownian motion, which results from the random collisions with the molecules of the surrounding fluid [9]. Though most of the mathematical reasoning and theoretical framework of conventional communication can be used for characterizing MC systems, there are, however, certain aspects of MC are fundamentally distinct from the EM communication.

In timing-based MC systems, the information to be transmitted is encoded in the time of release of information molecules [10]. Once released in the fluid medium, an information molecule takes a random path to the receiver. In diffusion-based molecular timing (DB-MT) channels, the random propagation delay associated with this random path acts as additive noise. The presence or absence of any drift in the fluid media significantly affects the nature of the additive noise term. In flow assisted environments where a positive drift is present in the fluid medium, this additive noise term is characterized by inverse Gaussian (IG) [11]. For drift free environments, this noise term follows a Lévy distribution [12]. Unlike the IG distribution with exponentially decaying tails, the Lévy distribution is α-stable having algebraic tails [13]. The stability of a Lévy distributed random variable results in the non-existence of finite moments, making it difficult to characterize and analyze the drift-free diffusive MC channels. To overcome this problem, the use of exponentially truncated Lévy statistics for obtaining the capacity bounds in diffusive molecular timing channel was first discussed in [14].

Manuscript received August 6, 2020; revised December 8, 2020; accepted January 18, 2021. Date of publication January 27, 2021; date of current version December 7, 2021. The work of Ranjan K. Mallik was supported in part by the Science and Engineering Research Board, a Statutory Body of the Department of Science and Technology, Government of India, under the J. C. Bose Fellowship. The associate editor coordinating the review of this article and approving it for publication was Y. Deng. *(Corresponding author: Nilay Pandey.)*

Gaurav Sharma and Ajay Singh are with the Department of Electrical Engineering, Indian Institute of Technology Jammu, Jagti, Jammu and Kashmir 181221, India (e-mail: 2018ree0018@iitjammu.ac.in; ajay.singh@iitjammu.ac.in).

Nilay Pandey and Ranjan K. Mallik are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110016, India (e-mail: nilaypandey03@gmail.com; rkmallik@ee.iitd.ernet.in).

Digital Object Identifier 10.1109/TMBMC.2021.3054907

The challenges of physical layer security at the nanoscale level were first highlighted by [15]. In particular, the authors discussed the concept of bio-chemical cryptography, wherein biological macro-molecule structure and configuration could be employed to keep up the information integrity. The potential research directions for using bio-chemical cryptography using observations from nature was discussed in [16]. The expressions for secrecy capacity in terms of thermodynamic transmitter power, the distance of eavesdropper, and the radius of the receiver was first calculated in [17]. The authors first considered the capacity expressions of [18] and then introduced the concept of eavesdropping in it. An Energy-Saving algorithm was implemented in [19], wherein secrecy was obtained using the Diffie-Hellman method. Further, a programmed biological entity modelling was adopted in [20], where two attack scenarios were considered. In [21] authors demonstrated the potential of accurate passive eavesdropper detection and localization in molecular communications. Authors used the attributes of the random-walk channel to detect an eavesdropper and then estimated its position accurately. A viable and low complexity physical layer security algorithm for secure molecular communications was highlighted in [22].

The transmission of information securely from the authorized transmitter (Alice) to the authorized receiver (Bob) has always been an essential consideration in any communication scenario [23]. In case of MC, the secure transmission of information becomes even more daunting given the limited computational capabilities of the nanodevices and the fact that the instantaneous channel state information (CSI) of eavesdropper (Eve) is not known to Alice for most practical scenarios. Since the information molecules in case of MC do not have the inherent capability to distinguish the receivers (both Bob and Eve), it becomes imperative to focus on secrecy whenever the predator receiver tries to retrieve sensitive information. In the case of MC, the computational and transmission capabilities of the devices involved is minimal, making the security introduced at the physical layer a handy, easy to implement tool to combat the menace of Eve as the random motion of the information molecules increases the probability of a molecule getting absorbed by Eve rather than by Bob.

In this work, we consider a purely diffusive molecular timing channel and derive the optimal design parameters (optimal secrecy and Bob's transmission rates) which would be useful for minimizing the generalized secrecy outage probability (GSOP), maximizing average fractional equivocation, and finally minimizing average information leakage rate. Although the secrecy performance metrics employed in this case are motivated from [24], where the performance of secrecy in quasi-static fading channels was discussed, the fundamental problem formulation and noise models considered in this work are different. The main contributions of this letter are as follows:

- Unlike [17], where the authors assume knowledge of the instantaneous CSI of Eve, in our case, the uniformly distributed distance of the eavesdropper means that there is no prerequisite knowledge about the CSI of Eve. As such, different secrecy performance metrics have been employed in this work.
- We first use the upper bound on the capacity given in [14] to obtain an approximate expression for the upper bound on the channel capacity. Based on this approximate expression, we calculate the transmission probability when eavesdropper distance is uniform distributed, which would be useful for calculating maximum achievable throughput, which is defined as probability of successful transmission of particles times the achievable secrecy rate.
- Using the throughput analysis, we calculate the optimal value of the secrecy rate and Bob's transmission rate.
- Based on the optimal design parameters values, we minimize GSOP, maximize average fractional equivocation and minimize the average information leakage rate, respectively.

The rest of the manuscript is organized as follows. Section II highlights the system model with a schematic diagram depicting an eavesdropping scenario. Section III illustrates various secrecy performance metrics and their implications on the system design. Section IV provides the numerical results which validate the system model, and finally, Section V concludes the paper.

Notation: The following notations would be used throughout the script: $\mathcal{U}(a, b)$ is a Uniformly distributed random variable (RV) over the interval [a, b] and ln(·), represents the natural logarithm. Random variables are represented by upper case letters like R, T_n, while their realization is represented using the respective lower case letters. $\frac{\partial}{\partial x}$ represents the partial differentiation of a function with respect to x. $h(X/Y)$ is equivocation which represents the differential entropy of X conditioned to the observed signal Y at the destination. We use $f_{Tn}(t_n)$ to represent the probability density function (PDF) of a continuous RV T_n. $\mathbb{P}(\cdot)$ denotes the probability. Expectation operator is denoted by $\mathbb{E}(\cdot)$. The Modified Bessel's function and incomplete Bessel or leaky aquifer function are represented as $K_v(z)$ and $K_v(x, y)$, respectively. Note that in this work, we use the terms information molecule and information particle interchangeably.

II. System Model

We consider the transmission of information from the authorized transmitter, Alice to a legitimate receiver, Bob over a diffusion-based molecular timing (DB-MT) channel, where the information to be transmitted is encoded in the time of release of the information molecule, in the presence of an eavesdropper, Eve. Fig. 1 represents this scenario of eavesdropping. For the sake of simplicity, we have considered a single particle system where Alice is a point source located at the origin ($x = 0$). Meanwhile, Bob and Eve are assumed to be absorbing receivers. Furthermore, the transmission occurs over a time-slotted channel with τ_m being the length of each time slot. In this work, the distance (d_E) of Eve from Alice is assumed to be uniform distributed. Let T_t be the time of release of an information molecule. After being released, each information molecule follows an independent and identically distributed

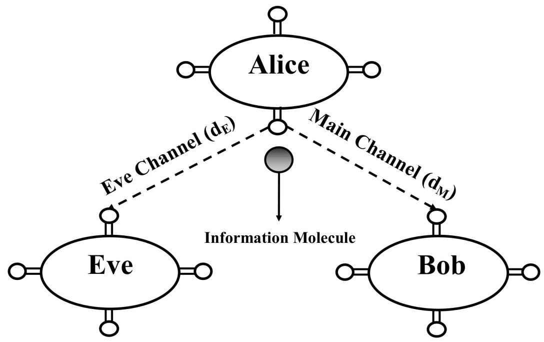

Fig. 1. Scenario of eavesdropping in Diffusion-based molecular communication.

(iid) propagation path and arrives at the receiver (either Bob or Eve) at time T_a. This arrival time is sum of T_t and random propagation delay T_n. Mathematically, it can be written as

$$T_a = T_t + T_n, \tag{1}$$

where $T_n = T_{n_B}$ if the information molecule arrives at Bob and $T_n = T_{n_E}$ if the information molecule arrives at Eve, with T_{n_B} and T_{n_E} being the random propagation time taken by an information particle to reach Bob and Eve, respectively. This propagation delay (T_n) for the drift free channel can be modeled as an α-stable Lévy distributed random variable (Lévy(μ, c)) [13]. The PDF of Lévy distributed RV *R* can be represented as

$$f_R(r;\mu,c) = \sqrt{\frac{c}{2\pi(r-\mu)^3}}\exp\left(-\frac{c}{2(r-\mu)}\right), \tag{2}$$

where μ is location parameter and *c* is scale parameter. In the case of a purely diffusive MC channel, the distance *d* between the transmitter and the receiver and the diffusion coefficient *D* of the information molecule in the given fluid media parametrize the scale parameter *c* (also called the Lévy noise parameter) which is given as

$$c = \frac{d^2}{2D}. \tag{3}$$

The additive noise term T_n can thus be written as $T_n \sim$Lévy$(0, d^2/(2D))$, i.e.,

$$f_{T_n}(t_n) = \frac{d}{\sqrt{4\pi D t_n^3}}\exp\left(-\frac{d^2}{4Dt_n}\right). \tag{4}$$

Once released in the fluid media, it is justified to assume that the information molecule undergoes degradation because of certain environmental factors. We adopt an exponential degradation model for the lifetime of the information molecules which can be modeled mathematically as [12]

$$h(\tau) = \alpha e^{-\alpha\tau}, \qquad \tau > 0, \tag{5}$$

where α is the *degradation parameter* and $h(\tau)$ is the exponentially decaying lifetime. Using this exponentially decay model, the truncated version of the first arrival time distribution, i.e., the truncated Lévy distribution is expressed as [14]

$$f_{t_d} = \begin{cases} 0, & \text{for } t_d \le 0 \\ k'\sqrt{\frac{d^2}{4\pi D t_d^3}}\,\mathrm{e}^{-\frac{d^2}{4Dt_d}}\,\mathrm{e}^{-\alpha t_d} & \text{for } t_d > 0, \end{cases} \tag{6}$$

where $k' = \exp(p)$ is the normalizing factor and p is a scaled version of the noise parameter given by $p = \sqrt{2\alpha c}$.

Note that, this exponentially degrading lifetime for the information molecules allows us to consider an inter-symbol interference (ISI) free channel for our analysis. Taking an approach similar to [12], we assume that the timing channel is divided into time slots of duration τ_m. In order to avoid any ISI τ_m is taken to be *sufficiently* large. A *sufficiently* large τ_m satisfies [12, eq. (7)]

$$\tau_m \gg \tau_x + \mathbf{E}(T_n), \tag{7}$$

where τ_x is the symbol interval within which a transmission can occur. For a given value of the parameter c, let L be a Bernoulli distributed RV with $L = 1$ for the case where the molecule arrives at the receiver within a time slot, such that $\Pr(L = 1) = p_\tau$ and $\Pr(L = 0) = 1 - p_\tau$, where $p_\tau = \Pr(T_n < \tau_n)$. In general, p_τ represents the hitting probability of the molecule. Using this formulation, the existing upper bound on the capacity of molecular timing channels as given by [14, eq. (38)] is taken. Compared to the most existing literature on molecular timing channels without drift, only the authors in [14] adopt a highly realistic exponential degradation model for the lifetime of the information molecules, which well models the natural decay of the molecules [25]. This leads to a totally new and complex mathematical analysis for the molecular timing channel which is, to the best of our knowledge, not reported elsewhere in the literature. This has motivated us to consider the exponentially truncated Lévy distribution as in [14]. Mathematically the capacity upper bound is expressed as

$$C_{ub} = \max_{\tau_x} \; p_\tau(\ln(\tau_x + \tau_n) - h(T_n|L=1)). \tag{8}$$

The hitting probability of the molecule p_τ is analytically derived in [14, eq. (32)] as

$$p_\tau = k'\sqrt{\frac{c}{2\pi}}\left(2\sqrt{\frac{p}{c}}K_{1/2}(p) - \sqrt{\frac{1}{\tau_n}}K_{1/2}\left(\alpha\tau_n, \frac{c}{2\tau_n}\right)\right). \tag{9}$$

From [14, eq. (38)] it is evident that for lower values of levy noise parameter the effect of logarithmic term in the upper bound on capacity is more prominent compared to other term. The expression of the capacity can be written as

$$C_{ub} \approx \frac{\ln(\tau_x + \tau_n)}{b} \approx \frac{\ln(\tau_m)}{b}, \tag{10}$$

where b is the scaling constant. Now by substituting the expression of τ_m from [12, eq.(7)] and putting $\tau_x = 1$ we have,

$$\begin{aligned}\ln(\tau_m) &\approx \ln\left(\tau_x + \mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{d^2}{4\alpha D}}\right) \\ &\approx \ln\left(\mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{d^2}{4\alpha D}}\right).\end{aligned} \tag{11}$$

The approximation is valid when $(\mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{d^2}{4\alpha D}})$ is small, i.e., ln$(1 + x) \approx$ ln(x) for small x. Thus, using properties of the logarithmic function and curve fitting techniques,

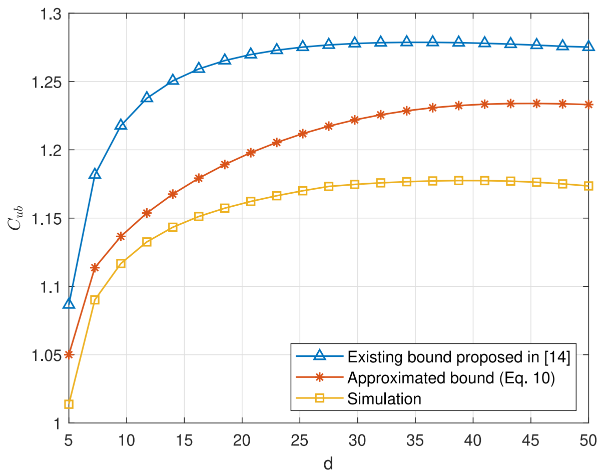

Fig. 2. Existing [14] and proposed approximate of upper bounds on the channel capacity, along with the simulation result for parameter values of $D = 500\mu m^2/s$ and $\alpha = 0.01 s^{-1}$. For all the simulation results in this letter, we have used particle based simulations, where the results are averaged over 30,000 independent realizations of the system.

the approximate solution for the upper bound on capacity is obtained as

$$C \approx \frac{1 + \ln(d) - \ln\left(\sqrt{4D\alpha}\right)}{b}. \tag{12}$$

As noted in [14, eq. (38)], the noise parameter $c = d^2/2D$ should be typically small for a purely diffusive MC channel so that the receiver does not need to wait for too long for the information molecule to arrive. Since D is a property of the system, a small value of c can be obtained by keeping the separation d between the transmitter and the receiver small. In this work too, we have considered small values for d. As can be observed from the capacity bound plots obtained in [14], for small values of the degradation parameter α, the capacity bound initially increases slightly with d, then decreases exponentially. Note that, our analysis holds for small values of d (which should be the case for any practical purely diffusive MC channel) for which the upper bound on capacity increases slightly with d. The validity of the approximation made in this work is confirmed using analytical as well as simulation plots obtained for small values of d as can be seen from Fig. 2 which shows the proposed approximation along with the existing expression for capacity upper bound [14, eq. (38)]. A close match of the proposed approximation and existing expression is seen from the figure.

For the sake of clarity, Eve's distance is expressed as d_E and Bob distance is denoted by d_M. Thus the expressions for channel capacities of Bob and Eve in terms of their respective distances from Alice are given by

$$C_B \approx \frac{1 + \ln(d_M) - \ln\left(\sqrt{4D\alpha}\right)}{b}, \tag{13}$$

$$C_E \approx \frac{1 + \ln(d_E) - \ln\left(\sqrt{4D\alpha}\right)}{b}. \tag{14}$$

In this work, the distances of neither Bob nor Eve are known at Alice and are assumed to be uniformly distributed. To validate the performance of our system model, we use the concept of throughput, which basically gives the information about the amount of confidential information propagated throughout the system. Mathematically, throughput is denoted as $\eta = P_{tx} R_S$, where R_S denotes achievable secrecy rate and P_{tx} represents the particle transmission probability from Alice. The transmission probability, also known as the hitting probability, can be interpreted as quality of service (QoS) measure, which in turn can be written as

$$P_{tx} = \mathbb{P}(R_B \le C_B), \tag{15}$$

where R_B denotes Bob's transmission rate while C_B represents the maximum achievable channel capacity for Bob. To guarantee whether transmission of particle from Alice is possible, the expression in (15) always holds true. Using (13) and assuming the distance of Bob to be uniformly distributed, i.e., $d_m \sim \mathcal{U}(0, \overline{d_M})$, the expression (15) is modified as

$$P_{tx} = \mathbb{P}\left(R_B \le \frac{A + \ln(d_M)}{b}\right) = \mathbb{P}\left(d_M \ge \mathrm{e}^{R_B b - A}\right), \tag{16}$$

where $A = 1 - \ln(\sqrt{4D\alpha})$. Using probability definition the expression (16) can be modified to be written as

$$P_{tx} = \int_{\mathrm{e}^{R_B b - A}}^{\overline{d_M}} \frac{1}{\overline{d_M}} dx = 1 - \frac{\mathrm{e}^{R_B b - A}}{\overline{d_M}}. \tag{17}$$

III. Secure Transmission Design

In this section, we optimize the secrecy performance of the system described in Section II. Since the instantaneous CSI of neither Bob nor Eve is known to Alice, it is very difficult to characterize the system in terms of exact secrecy. One way to characterizing the secrecy performance of the system is to use a performance metric such as the secrecy outage probability (SOP). However, the classical SOP has certain constraints which sometimes are too stringent for practical systems, and a system designer will find it very difficult to adopt the optimal design parameters based on the classical SOP, as the resulting conditions are too stringent for any practically feasible system. Moreover, the classical SOP neither gives information about Eve's decodability nor does it give the rate at which confidential information is leaked to Eve. To overcome these limitations of the classical SOP, we use newer secrecy metrics such as GSOP, average fractional equivocation, and average information leakage rate. These secrecy performance metrics give insights about how information integrity is maintained when the instantaneous CSI of Eve is not known to Alice. In this work, we study the optimal values for the secrecy and Bob's rate, which minimizes the GSOP, maximizes the average fractional equivocation, and minimizes average information leakage rate.

We then examine the significance of the proposed secrecy metrics from the perspective of a system designer. The proposed secrecy metrics lead to different optimal system design parameters as compared to the optimal parameters obtained using the classical SOP. Furthermore, the optimal transmission design based on the classical SOP results in a large secrecy loss, if the actual system requires a low decodability at the eavesdropper or a low information leakage rate. It is interesting to note that by adopting the optimal design based on the classical SOP would lead to a large secrecy loss when the secrecy performance is measured in terms of the secrecy metrics used in this letter.

In a practical scenario where partial secrecy is experienced, the maximum achievable fractional equivocation is given mathematically as eq. (17) [24]

$$\Delta = \begin{cases} 1, & \text{for } C_E \le C_B - R_S \\ \frac{C_B - C_E}{R_S}, & \text{for } C_B - R_S < C_E < C_B \\ 0, & \text{for } C_B \le C_E. \end{cases} \tag{18}$$

Since $R_B \le C_B$ can be represented by (13) and C_E can be represented by (14), the fractional equivocation in terms of Eve's distance can be modified as

$$\Delta = \begin{cases} 1, & \text{for } d_E \le \mathrm{e}^{R_B b - R_S b - A} \\ \frac{R_B b - \ln(d_E) - A}{R_S}, & \text{for } \mathrm{e}^{R_B b - R_S b - A} < d_E < \mathrm{e}^{R_B b - A} \\ 0, & \text{for } \mathrm{e}^{R_B b - A} \le d_E. \end{cases} \tag{19}$$

The expression for the GSOP is given by

$$P_{out} = \mathbb{P}(\Delta < \phi), \tag{20}$$

where ϕ is the minimum value of the fractional equivocation which varies from 0 to 1 ($0 < \phi < 1$). The expression for the GSOP when Eve's distance is uniformly distributed ($\mathcal{U}(0, \overline{d_E})$) is given by

$$\begin{aligned} P_{out} &= \mathbb{P}\Big(d_E \ge \mathrm{e}^{R_B b - A}\Big) \\ &\quad + \mathbb{P}\Big(\mathrm{e}^{R_B b - R_S b - A} < d_E < \mathrm{e}^{R_B b - A}\Big) \\ &\quad \times \mathbb{P}\Bigg(\frac{R_B b - \ln(d_E) - A}{R_S} \\ &\qquad < \phi | \mathrm{e}^{R_B b - R_S b - A} < d_E < \mathrm{e}^{R_B b - A}\Bigg) \\ &= 1 - \frac{\mathrm{e}^{R_B b - R_S \phi - A}}{\overline{d_E}}. \end{aligned} \tag{21}$$

To minimize the GSOP subject to $\eta \ge \Gamma$ and $R_B \ge R_S > 0$, the optimization problem can be written as

$$\begin{aligned} \min_{R_B, R_S} \quad & P_{out} = 1 - \frac{\mathrm{e}^{R_B b - R_S \phi - A}}{\overline{d_E}}, \\ \text{s.t.} \quad & \eta \ge \Gamma, \; R_B \ge R_S > 0. \end{aligned} \tag{22}$$

The average fractional equivocation is given as

$$\bar{\Delta} = \mathbb{E}(\Delta). \tag{23}$$

The average fractional equivocation gives an intuitive insight on the overall decoding error probability of Eve and is expressed as

$$\bar{\Delta} = \int_0^{\lambda} \frac{1}{\overline{d_E}} \, dx + \int_{\lambda}^{\lambda_1} \frac{1}{\overline{d_E}} \left(\frac{R_B b - \ln(x) - A}{R_S}\right) dx. \tag{24}$$

This results in

$$\begin{aligned} \bar{\Delta} &= \frac{\lambda}{\overline{d_E}} + \left(\frac{R_B b - A}{R_S b \overline{d_E}}\right)(\lambda_1 - \lambda) \\ &\quad - \left(\frac{\lambda_1 \ln(\lambda_1) - \lambda_1 - \lambda \ln(\lambda) + \lambda}{R_S b \overline{d_E}}\right), \end{aligned} \tag{25}$$

where λ=$\mathrm{e}^{R_B b - R_S b - A}$ and λ_1=$\mathrm{e}^{R_B b - A}$. Similar to the optimization problem of the GSOP, the optimization problem for the maximization of the average fractional equivocation $\bar{\Delta}$ subject to $\eta \ge \Gamma$ and $R_B \ge R_S > 0$ can be expressed as

$$\begin{aligned} \max_{R_B, R_S} \quad & \frac{\lambda}{\overline{d_E}} + \left(\frac{R_B b - A}{R_S b \overline{d_E}}\right)(\lambda_1 - \lambda) - \frac{\lambda_1 \ln(\lambda_1)}{R_S b \overline{d_E}} \\ & + \frac{\lambda_1}{R_S b \overline{d_E}} + \frac{\lambda \ln(\lambda)}{R_S b \overline{d_E}} - \frac{\lambda}{R_S b \overline{d_E}}, \\ \text{s.t.} \quad & \eta \ge \Gamma, \, R_B \ge R_S > 0. \end{aligned} \tag{26}$$

Furthermore, the average information leakage rate, which gives information about the amount and the rate at which confidential information is leaked to Eve, is given by

$$R_L = \mathbb{E}\{(1 - \Delta) R_S\} = \big(1 - \bar{\Delta}\big) R_S. \tag{27}$$

Using (25), the average information leakage rate R_L for the case when Eve's distance is uniformly distributed simplifies to

$$\begin{aligned} R_L = R_s &- \frac{\lambda(R_s b + \ln(\lambda) - R_B b + A - 1)}{b \overline{d_E}} \\ &- \frac{\lambda_1 (R_B b - \ln(\lambda_1) - A + 1)}{b \overline{d_E}}. \end{aligned} \tag{28}$$

Thus, the optimization problem which minimizes the average information leakage rate R_L subject to $\eta \ge \Gamma$ and $R_B \ge R_S > 0$ is obtained as

$$\begin{aligned} \min_{R_B, R_S} \quad & R_s - \frac{\lambda(R_s b + \ln(\lambda) - R_B b + A - 1)}{b \overline{d_E}} \\ & - \frac{\lambda_1 (R_B b - \ln(\lambda_1) - A + 1)}{b \overline{d_E}}. \\ \text{s.t.} \quad & \eta \ge \Gamma, \; R_B \ge R_S > 0. \end{aligned} \tag{29}$$

The required throughput constraint cannot be achieved when Γ is more than the maximum achievable throughput (when $R_B \ge R_S > 0$). Therefore, to maximize η, where

$$\eta = R_S - \frac{R_S \mathrm{e}^{R_B b - A}}{\overline{d_M}}, \tag{30}$$

the optimization problem in (29) can be reformulated as

$$\begin{aligned} \max_{R_B, R_S} \quad & R_S - \frac{R_S \mathrm{e}^{R_B b - A}}{\overline{d_M}}. \\ \text{s.t.} \quad & R_B \ge R_S > 0. \end{aligned} \tag{31}$$

For any value of R_S, the partial derivative $\partial \eta / \partial R_B$ is always negative. Thus for maximizing η subject to $R_S > 0$ and $R_B = R_S$, the optimization problem of (31) becomes

$$\begin{aligned} \max_{R_S} \quad & R_S - \frac{R_S \mathrm{e}^{R_S b - A}}{\overline{d_M}}. \\ \text{s.t.} \quad & R_S > 0. \end{aligned} \tag{32}$$

Taking the partial derivative of (32) w.r.t. R_S, we get

$$\frac{\partial \eta}{\partial R_S} = 1 - \frac{\mathrm{e}^{R_S b - A}}{\overline{d_M}} - \frac{b R_S \mathrm{e}^{R_S b - A}}{\overline{d_M}}. \tag{33}$$

By putting $\frac{\partial \eta}{\partial R_S}$=0, we get the optimal R_S, denoted by $R_S^{\square}$, as

$$R_S^{\square} = \frac{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right) - 1}{b}, \tag{34}$$

where $\mathrm{W}_0(\cdot)$ denotes the principal branch of the Lambert W function. Substituting (34) in (32), the range of the throughput can be obtained as

$$0 \le \eta \le \left(\frac{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right) - 1}{b}\right)\left(1 - \frac{\mathrm{e}^{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right) - 1 - A}}{\overline{d_M}}\right). \tag{35}$$

For the throughput to have the maximum value, the optimum range of the secrecy rate R_S needs to be calculated. The acceptable range for which the throughput is maximum is $R_{s,min} \le R_S \le R_{s,max}$. Moreover, the optimum value of Bob's rate for which the throughput of the system is maximized can be obtained from (31) and is given by

$$R_B^* = \frac{1}{b}\left(A + \ln\left(\overline{d_M} - \frac{\overline{d_M}\eta_{max}}{R_S^*}\right)\right), \tag{36}$$

where η_{max} is expressed as

$$\eta_{max} = \left(\frac{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right) - 1}{b}\right)\left(1 - \frac{\mathrm{e}^{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right) - 1 - A}}{\overline{d_M}}\right). \tag{37}$$

This R_B^* is different for different R_S^*. Now, according to (22), in order to minimize the GSOP, we need to maximize

$$F_1 = R_B b - R_S \phi - A. \tag{38}$$

Therefore, by substituting (36) in (38) and differentiating w.r.t. R_S, we get

$$\phi = \frac{\overline{d_M}\eta_{max}}{R_S\left(\overline{d_M}R_S - \overline{d_M}\eta_{max}\right)}. \tag{39}$$

Using ϕ, the optimal secrecy rate R_{s1}^* which minimizes the GSOP is obtained as

$$R_{s1}^* = \frac{\eta_{max}\phi + \sqrt{\eta_{max}^2\phi^2 + 4\phi\eta_{max}}}{2\phi}. \tag{40}$$

Thus, Bob's optimal rate R_{B1}^* can be obtained by substituting (40) in (36). Similarly, the optimal secrecy rate R_{s2}^* and Bob's optimal rate R_{B2}^* which maximize the average fractional equivocation $\bar{\Delta}$, subject to $R_{s,min} \le R_S \le R_{s,max}$ can be obtained after solving the maximization problem as given in (26). The optimization problem in (26) can be rewritten as

$$\begin{aligned} &\max_{R_S} \ \frac{\mathrm{e}^{R_B b - A}\left(1 - \mathrm{e}^{-R_S b}\right)}{b R_S \overline{d_E}}. \\ &\text{s.t.} \ \ R_{s,min} \le R_S \le R_{s,max}. \end{aligned} \tag{41}$$

Here maximizing $\bar{\Delta}$ requires maximizing

$$F_2 = \frac{\mathrm{e}^{R_B b - A}\left(1 - \mathrm{e}^{-R_S b}\right)}{b R_S \overline{d_E}}. \tag{42}$$

Now, for any R_s, Bob's optimal rate R_{B2}^* which maximizes the throughput and the average fractional equivocation is same as that obtained in (36). By putting R_{B2}^* in (41), the optimization problem which maximizes the average fractional equivocation $\bar{\Delta}$ subject to $R_{s,min} \le R_S \le R_{s,max}$ can be modified as

$$\begin{aligned} &\max_{R_S} \ \frac{\left(\overline{d_M}R_S - \overline{d_M}\eta_{max}\right)\left(1 - \mathrm{e}^{-R_S b}\right)}{b R_S^2 \overline{d_E}}. \\ &\text{s.t.} \ \ R_{s,min} \le R_S \le R_{s,max}. \end{aligned} \tag{43}$$

From (43), it can be observed that a closed form expression for R_{S2}^* is mathematically intractable. Thus, obtaining R_{S2}^* becomes a numerical optimization problem which can be solved by implementing the golden section search (GSS) technique. Furthermore, based on (29), the minimization of the average information leakage rate is accomplished by maximizing the average fractional equivocation, since the solution R_{S3}^* to the optimization problem is mathematically intractable. Thus, the optimal secrecy rate R_{S3}^* which minimizes the average information leakage rate can be obtained by employing the GSS technique.

Remark: Note that the above analysis for the uniform case can be extended to the non-uniform case also by simply modifying the expressions for the transmission probability (P_{tx}), the outage probability (P_{out}), the average fractional equivocation ($\bar{\Delta}$), and the average information leakage rate (R_L). Based on these newfound expressions, one can obtain the optimal secrecy and Bob's transmission rates which minimize P_{out}, maximize $\bar{\Delta}$, and minimize R_L of the system.

IV. Numerical Results

Based on the mathematical analysis presented in the previous section, in this section, we present the numerical results for the proposed system model to validate the effect of optimal secrecy rate and optimal transmission rate for Bob that would minimize generalized secrecy outage, maximize average fractional equivocation and finally minimize average information leakage rate respectively. The optimum range of throughput constraint as obtained by (35) is $0 \le \eta \le 0.16$ bits/s with $\alpha = 0.01 s^{-1}$ and $D = 500 \mu m^2/s$. Using the η range, we first analyze the optimal secrecy rate that optimizes various secrecy performance metrics.

Fig. 3 shows the plot of the optimal secrecy rate R_S^* versus the throughput constraint η. As shown in the plot the values of different optimal secrecy rate parameters (R_{S1}^*, R_{S2}^* and R_{S3}^*) are obtained by minimizing GSOP, maximizing average fractional equivocation and minimizing average information leakage rate respectively. Since R_{S1}^*, R_{S2}^* and R_{S3}^* are distinct from each other, they have different optimal ranges. As shown in the figure, the optimal range of R_{S1}^* which minimizes GSOP is 0.0142 to 0.4780 bits/s, while to maximize average fractional equivocation the optimal range of R_{S2}^* is

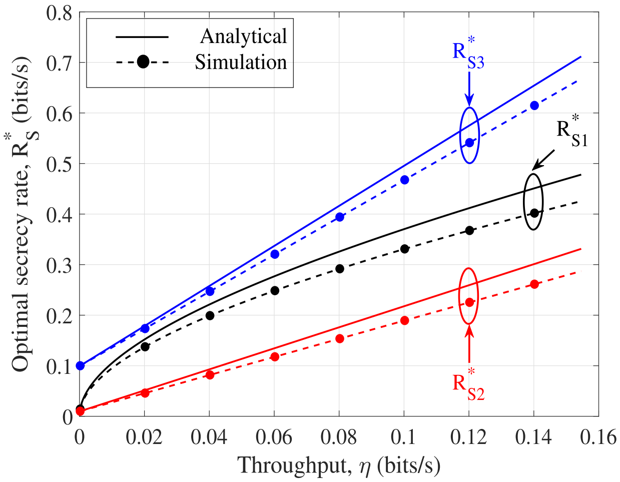

Fig. 3. Optimal secrecy rate versus throughput for different secrecy performance metrics. The other parameters are $\phi = 1$, $\overline{d_M} = 50\mu m$ and $\overline{d_E} = 50\mu m$.

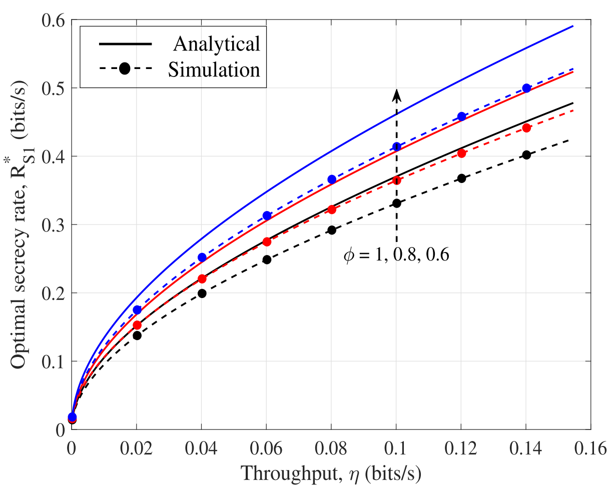

Fig. 4. Optimal secrecy rate versus throughput for GSOP for different fractional equivocation (ϕ). The other parameters are $\overline{d_M} = 50\mu m$ and $\overline{d_E} = 50\mu m$.

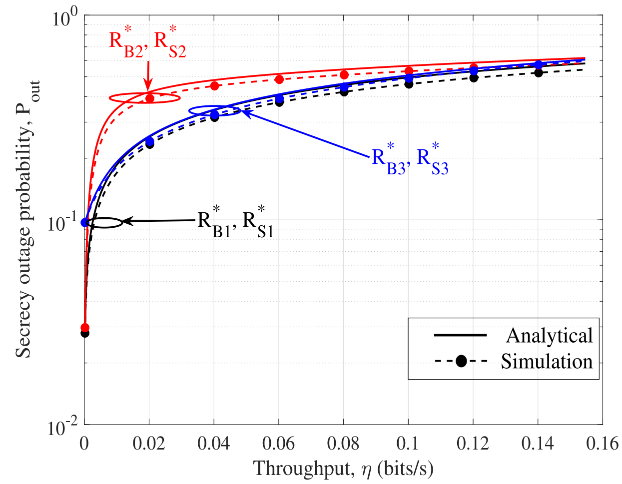

Fig. 5. Secrecy outage probability versus throughput. The other parameters are $\phi = 1$, $\overline{d_M} = 50\mu m$, and $\overline{d_E} = 50\mu m$.

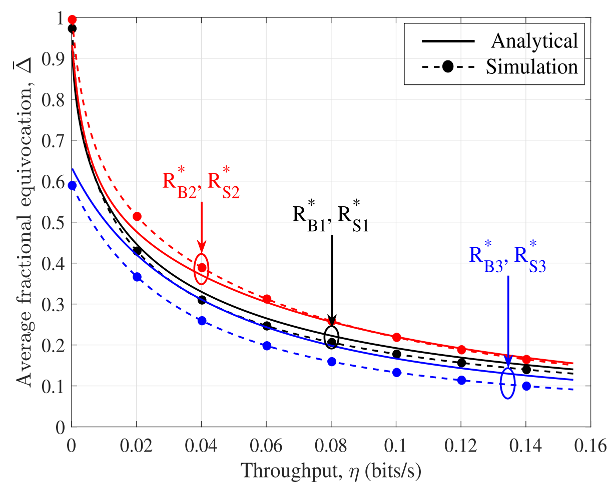

Fig. 6. Average fractional equivocation versus throughput. The other parameters are $\phi = 1$, $\overline{d_M} = 50\mu m$, and $\overline{d_E} = 50\mu m$.

0.0100 to 0.3316 bits/s, and finally in order to minimize average information leakage rate the optimal range of R^*_{S3} is 0.10 to 0.6684 bits/s. Moreover, the optimal transmission rate for Bob (R^*_B) as represented by (36) is distinct for all the three optimization scenarios and is represented as R^*_{B1}, R^*_{B2} and R^*_{B3}. From the figure it can also be noted that the distinct values of R^*_{S1}, R^*_{S2} and R^*_{S3} is the primary reason for the distinct values of the optimal transmission rates of Bob (R^*_{B1}, R^*_{B2} and R^*_{B3}). Thus from the plot, it is evident that by employing different secrecy metrics to evaluate the secrecy performance, the optimal design parameters are different.

The variation of optimal secrecy rate, R^*_{s1}, which basically minimizes the GSOP, is shown in Fig. 4 as a function of throughput for different values of fractional equivocation, ϕ. From the figure it can be observed that as the level of ϕ decreases, R^*_{S1} increases minimizing the GSOP. Furthermore, based on the analytical results obtained in the preceding section, we have obtained three different optimal design parameter pairs: R^*_{B1}, R^*_{S1} are the optimal design parameters for minimizing GSOP, R^*_{B2}, R^*_{S2} are the optimal design parameters for maximizing average fractional equivocation, and R^*_{B3}, R^*_{S3} are the optimal design parameters that minimize average information leakage rate.

The effect of secrecy outage probability with variation in throughput constraint, for different values of optimal design parameter pairs (R^*_{B1}, R^*_{S1}), (R^*_{B2}, R^*_{S2}) and (R^*_{B3}, R^*_{S3}) is shown in Fig. 5. It can be observed from the SOP plot that increasing the throughput constraint increases the SOP of the system. This is primarily because of the fact that as the throughput of the system is increased, the probability of the particle getting absorbed at Eve increases. Furthermore, the effect of different optimal rate design parameters on the SOP plot can also be observed in the figure.

Fig. 6 presents the plot for average fractional equivocation as a function of throughput for different optimal rate design parameter pairs (R^*_{B1}, R^*_{S1}), (R^*_{B2}, R^*_{S2}), and (R^*_{B3}, R^*_{S3}). From the figure, it is evident that increasing throughput decreases average fractional equivocation. The plot also shows

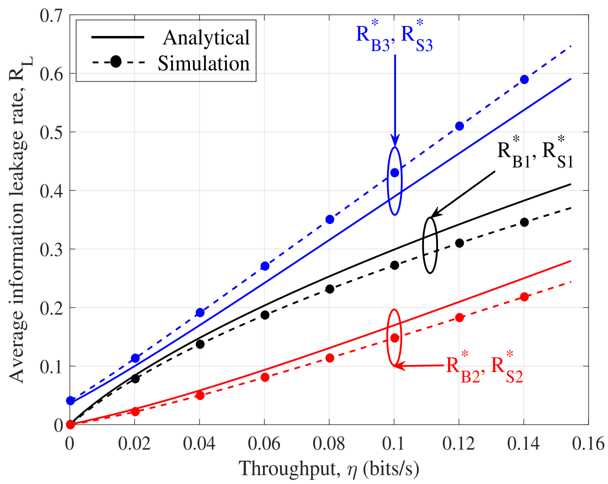

Fig. 7. Average information leakage rate versus throughput. The other parameters are $\phi = 1$, $\overline{d_M} = 50\mu m$, and $\overline{d_E} = 50\mu m$.

that though the transmission with R_{B2}^* and R_{s2}^* maximizes average fractional equivocation, the system's performance also suffers from higher SOP at the same time.

The plot showing average information leakage rate versus throughput for different design parameter pairs (R_{B1}^*, R_{S1}^*), (R_{B2}^*, R_{S2}^*), and (R_{B3}^*, R_{S3}^*), is shown in Fig. 7. From the plot, it can be easily inferred that increasing throughput causes the average information leakage rate to increase. This is perhaps because of the fact that increasing throughput increases the particle's probability of getting absorbed at Eve. Additionally, transmission with R_{B3}^* and R_{S3}^* not only increases the average information leakage rate but it also simultaneously increases SOP and decreases average fractional equivocation, respectively.

From the Fig. 5, Fig. 6 and Fig. 7 it is also apparent that using R_{B1}^* and R_{S1}^* as the optimal design parameter not only minimizes GSOP but it also leads to a significant loss when the system's requirement is to maximize average fractional equivocation or to minimize average information leakage. Similarly, using R_{B2}^* and R_{S2}^* as the optimal design parameter for the system's design undoubtedly maximizes average fractional equivocation and minimizes the average information leakage, but it significantly deteriorates in terms of GSOP. Lastly, using R_{B3}^* and R_{S3}^* as the optimal design parameter, the system not only suffers from lower fractional equivocation, but it also suffers from higher average information leakage rate. Thus from the observations, it is evident that for a particular optimal design parameter value, there is always a trade-off between various secrecy performance metrics of the system.

V. Conclusion

In this letter, we have investigated the optimal secrecy and Bob's optimal transmission rates in order to minimize the GSOP, maximize the average fractional equivocation, and minimize the average information leakage rate, respectively. Expressions for optimal values of design parameters which characterize the performance of the system were obtained and analyzed for various secrecy performance metrics. Based on the optimal design parameters, we obtained the corresponding numerical results. From the numerical results, it can be inferred that there is always a trade-off between different optimal design parameters which not only minimize the secrecy outage probability and maximize the average fractional equivocation but also minimize the average information leakage rate.

This analysis of secrecy optimization will help bridge the gap between theoretical and practical aspects of the secrecy in MC systems. We expect this analysis to serve as a basis for our future research involving more complex, multi-particle MC systems.

References

[1] W. Guo, C. Mias, N. Farsad, and J.-L. Wu, "Molecular versus electromagnetic wave propagation loss in macro-scale environments," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 1, no. 1, pp. 18–25, Mar. 2015.

[2] N. Farsad, H. B. Yilmaz, A. Eckford, C.-B. Chae, and W. Guo, "A comprehensive survey of recent advancements in molecular communication," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1887–1919, 3rd Quart., 2016.

[3] Y. Murin, N. Farsad, M. Chowdhury, and A. Goldsmith, "Communication over diffusion-based molecular timing channels," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[4] I. F. Akyildiz, F. Brunetti, and C. Blázquez, "Nanonetworks: A new communication paradigm," *Comput. Netw.*, vol. 52, no. 12, pp. 2260–2279, 2008.

[5] B. Atakan, O. B. Akan, and S. Balasubramaniam, "Body area nanonetworks with molecular communications in nanomedicine," *IEEE Commun. Mag.*, vol. 50, no. 1, pp. 28–34, Jan. 2012.

[6] M. S. Kuran, H. B. Yilmaz, T. Tugcu, and I. F. Akyildiz, "Modulation techniques for communication via diffusion in nanonetworks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.

[7] N. Pandey, R. K. Mallik, and B. Lall, "Molecular communication: The first arrival position channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 508–511, Apr. 2019.

[8] N. Farsad, W. Guo, and A. W. Eckford, "Tabletop molecular communication: Text messages through chemical signals," *PloS one*, vol. 8, no. 12, 2013, Art. no. e82935.

[9] J. Crank, *The Mathematics of Diffusion*. Oxford, U.K.: Oxford Univ. Press, 1979.

[10] H. Zhai, L. Yang, T. Nakano, Q. Liu, and K. Yang, "Bio-inspired design and implementation of mobile molecular communication systems at the macroscale," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[11] K. V. Srinivas, A. W. Eckford, and R. S. Adve, "Molecular communication in fluid media: The additive inverse Gaussian noise channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4678–4692, Jul. 2012.

[12] N. Pandey, R. K. Mallik, and B. Lall, "Truncated lévy statistics for diffusion based molecular communication," in *Proc. IEEE Global Commun. Conf.*, 2017, pp. 1–6.

[13] N. Farsad, W. Guo, C.-B. Chae, and A. Eckford, "Stable distributions as noise models for molecular communication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2015, pp. 1–6.

[14] N. Pandey, R. K. Mallik, and B. Lall, "Performance analysis of diffusive molecular timing channels," *IET Commun.*, vol. 13, no. 18, pp. 3059–3067, Nov. 2019.

[15] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Commun. Netw.*, vol. 3, no. 3, pp. 151–160, 2012.

[16] 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.

[17] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, and M. Pierobon, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, pp. 110687–110697, 2019.

[18] 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.

[19] S. R. Islam, F. Ali, H. Moon, and K.-S. Kwak, "Secure channel for molecular communications," in *Proc. Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, 2017, pp. 1–4.
[20] 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. 2015.
[21] W. Guo, Y. Deng, B. Li, C. Zhao, and A. Nallanathan, "Eavesdropper localization in random walk channels," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1776–1779, Sep. 2016.
[22] W. Guo, Z. Wei, and B. Li, "Secure Internet-of-Nano Things for targeted drug delivery: Distance-based molecular cipher keys," in *Proc. IEEE 5th Middle East Africa Conf. Biomed. Eng. (MECBME)*, 2020, pp. 1–6.
[23] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[24] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016.
[25] T. Nakano, Y. Okaie, and J.-Q. Liu, "Channel model and capacity analysis of molecular communication with brownian motion," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 797–800, Jun. 2012.

Gaurav Sharma (Graduate Student Member, IEEE) received the B.Tech. degree in electronics and communication from Jammu University, Jammu and Kashmir, India, in 2014, and the M.Tech. degree in electronics and communication from Shri Mata Vaishno Devi University, Jammu and Kashmir, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Indian Institute of Technology Jammu, Jammu and Kashmir. From December 2017 to March 2018, he was a project intern at one of the DRDO laboratory, ANURAG, Hyderabad. His research interests include molecular communication and physical layer security.

Nilay Pandey (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Graphic Era University, India, in 2012, the M.Tech. degree in signal and image processing from the National Institute of Technology, Rourkela, India, in 2014, and the Ph.D. degree from the Bharti School of Telecommunication Technology and Management, Indian Institute of Technology Delhi, New Delhi, India, in 2020. From July 2014 to March 2015, he was a Senior Research Fellow, working on a project with the Department of Atomic Energy, India. He is currently working as an Early-Doc Research Fellow with the Department of Electrical Engineering, Indian Institute of Technology Delhi. His research interests include molecular communication, MIMO radar, signal and image processing, and machine learning.

Ajay Singh (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Kurukshetra University, Kurukshetra, India, in 2003, and the M.E. degree in electronics and communication engineering from Panjab University, Chandigarh, India, in 2007, and the Ph.D. degree from the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India, in 2012. From May 2013 to January 2016, he was a faculty member with the Department of Electronics and Communication Engineering, National Institute of Technology Raipur, Chhattisgarh, India. From January 2016 to March 2018, he was a Faculty Member with the Department of Electronics and Communication Engineering, National Institute of Technology Hamirpur, Hamirpur, India, on leave from the National Institute of Technology Raipur, Raipur, India. Since March 2018, he has been a faculty member with the Department of Electrical Engineering, Indian Institute of Technology Jammu, Jammu and Kashmir, India, where he is currently an Assistant Professor. His current research interests are in physical layer security, wireless powered communications and molecular communications.

Ranjan K. Mallik (Fellow, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology Kanpur, Kanpur, in 1987, and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, in 1988 and 1992, respectively.

From August 1992 to November 1994, he was a Scientist with the Defence Electronics Research Laboratory, Hyderabad, India, working on missile and EW projects. From November 1994 to January 1996, he was a Faculty Member with the Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology Kharagpur, Kharagpur, India. From January 1996 to December 1998, he was with the faculty with the Department of Electronics and Communication Engineering, Indian Institute of Technology Guwahati, Guwahati, India. Since December 1998, he has been with the faculty with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India, where he is currently an Institute Chair Professor. His research interests are in diversity combining and channel modeling for wireless communications, space-time systems, cooperative communications, multiple-access systems, power line communications, molecular communications, difference equations, and linear algebra.

Dr. Mallik is a recipient of the Hari Om Ashram Prerit Dr. Vikram Sarabhai Research Award in the field of electronics, telematics, informatics, and automation, the Shanti Swarup Bhatnagar Prize in engineering sciences, the Khosla National Award, and the J. C. Bose Fellowship. He has served as an Area Editor and an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS. He is also a member of the IEEE Communications, Information Theory, and Vehicular Technology Societies, the American Mathematical Society, and the International Linear Algebra Society; a fellow of the IEEE, the Indian National Academy of Engineering, the Indian National Science Academy, The National Academy of Sciences, India, Prayagraj, the Indian Academy of Sciences, Bengaluru, The World Academy of Sciences-for the advancement of science in developing countries (TWAS), The Institution of Engineering and Technology, U.K., The Institution of Electronics and Telecommunication Engineers, India, and The Institution of Engineers (India); and a Life Member of the Indian Society for Technical Education. He is a member of Eta Kappa Nu.