Secrecy performance of diffusion based molecular timing channels

Gaurav Sharma | Ajay Singh

Department of Electrical Engineering, Indian Institute of Technology Jammu, Jammu and Kashmir, India

Correspondence
Gaurav Sharma, Department of Electrical Engineering, Indian Institute of Technology Jammu, Jammu and Kashmir, India.
Email: 2018ree0018@iitjammu.ac.in

Abstract
Motivated by the study of security issues in molecular communication, this paper addresses the problem of secure communication in a bio-inspired field where confidentiality of the information is of significant importance. The new metrics are used for the secrecy analysis where eavesdropper’s decodability of confidential message and amount of information leakage is taken into account, which is not considered using conventional secrecy outage probability. A diffusion-based molecular communication system is considered where the information to be transmitted is the time of release of the molecules. Typically in the existing literature in molecular timing channels, the position of the eavesdropper is known, which is usually an impractical assumption. If no information about eavesdropper is known, it could be located at any distance with probability distribution be assumed to be uniform and Gaussian. In this paper, the closed-form expressions for the eavesdropper capacity, generalised secrecy outage probability, average fractional equivocation and average information leakage rate have been obtained when the eavesdropper is located at a random distance from the transmitter.

1 | INTRODUCTION

Molecular Communication (MC), being a multifaceted exploratory area is extravagantly found in telecommunications, computer sciences and microbiology [1–3]. Since this research area has been principally pointed out in the naturally occurring organisms; thus, the technological breakthrough compelled the development of this bio-inspired man-made communication system’s [4, 5]. Basically, molecular communication is installed into the environment where there is difficulty in the utilisation of the conventional methodology [6–8]. The telecommunication engineers look at MC as a communication prototype, where information propagates from the transmitter to the receiver with the help of chemical reactions and molecule transport [9–11]. Not all the molecules that are journeying the fluidic environment reach the receiver [12, 13]. A considerable amount of molecules are degraded and are lost in their voyage. Leftover molecules that reach the receiver undergo chemical transformation and form bonds with the ligand receptors prevalent on the surface of the receiver.

In number and timing-based modulation approaches, information is encompassed in the number and time of the release of molecules, which are dispatched from the transmitter to the receiver in the form of chemical pulses [14, 15]. Practically, the timing-based modulation is observed inside the synaptic cleft of the human brain [16]. This timing-based approach wherein two chemical synapses communicate over a chemical channel as illustrated in [17] is based on the assumption, which is valid for the case of perfect absorbing materials, that the molecule, when detected by the receiver, is removed from the environment thereby preventing inter symbol interference [18]. Moreover, the modulation of information molecules on the time of release is analogous to pulse position modulation technique. Since its inception, MC has found ever-increasing growth in the past decade wherein the majority of the work is focused on the information-theoretic aspects [19]. Subsequently, many experimental setups capable of transmitting messages at a comparatively low bit rate have been proposed in the past few years which signifies the practicality of this field [20].

Moreover, the transmission of information securely from the transmitter to the receiver has always been a vital characteristic aspect in a communication systems scenario [9, 11, 21]. Thus the concept of secure transmission becomes imperative to be used in this fairly new field of communication since there is a propagation of privacy-sensitive information from the transmitter to the receiver [22]. Additionally, the elemental study of secure

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2020 The Authors. IET Communications published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology
communication at the early stage of molecular communication is somewhat easier than the analysis done after a considerable headway has been accomplished in this promising technology. Alternatively, in the timing based MC, the transmitted information bits are encoded at the time of the release of molecules [23]. Truncated Lévy statistics used for obtaining the capacity bounds (Upper as well as Lower) in the diffusion-based molecular communication channel, was first discussed in [6].

However, the concept of secure communication in molecular communication was first highlighted in [9], wherein the challenges of physical layer security at the nano-scale level were presented. To maintain the information, architectural and structural integrity of the biological entity, the concept of biochemical cryptography was implemented. Such, bio-chemical cryptography derived its basis from the human immune system, which was considered in [10]. The closed-form expression for the secrecy capacity was calculated in [11], wherein the secrecy capacity was dependent on the thermodynamic transmitter power, distance of eavesdropper, bandwidth of information signal and the radius of the receiver. Likewise, the closed-form expression of channel capacity while considering the channel memory and molecular noise was undertaken in [19]. For the molecular noise, particle’s location displacement was considered, and for channel memory, Fick’s Diffusion principles were considered. For secure communication, Energy-Saving algorithm was implemented in [22], wherein secrecy was obtained by the Diffie–Hellman method. The concept of programmed biological entities modelling along with the cooperative motility and chemical sensing for the cellular entity was examined in [24]. Here, the authors considered two attack scenarios while taking into consideration some countermeasure strategies.

1.1 Motivation

The fundamental requirement lies in the elementary modelling of highly complex diffusion-based molecular communication systems which would then be employed for secure communication. As based on the aforementioned literature, nowadays, MC is looked up as a promising field of research. Wherein, its numerous parameters are being adopted for the implementation, interfacing and coordination of the Biological systems into those environments where the present existing technologies have major limitations. In molecular communication there are basically two eavesdropping scenarios: Blackhole attack where malicious node attract the molecule towards itself (by emitting chemo-attractants), Sentry attacks where a malicious node in the vicinity of the target cells emit chemo-repellents not letting the molecule to reach the legitimate node; thus usage of secrecy for information transfer becomes vital. As the primary application of this bio-inspired field is in human healthcare; thus, it becomes imperative for the system to have robustness in terms of secure information transfer.

As a matter of fact, recently physical layer security has also drawn the attention of the researchers since there is no prerequisite requirement of the computational power of the eavesdropper. Since in this new paradigm, the computational power of the devices is limited (because of large energy constraints) thus the security at the physical layer becomes a handy tool to combat the menace of an eavesdropper. Moreover, to illustrate this issue, we have considered the scenario in which the exact distance of the eavesdropper from the authorised transmitting point source is not known, but there is some knowledge in terms of its mean and variance values. Since the motion of the particles in the media is random, so the chances that a particle being received at eavesdropper (Eve) becomes highly probable. As a result, in the first scenario, we have modelled the eavesdropper distance as a uniform distributed random variable, and in the second case, the eavesdropper distance modelling is assumed to be Gaussian distributed with certain mean and variance. Using maximum likelihood principle with sampled observations, we can estimate the mean and variance of the wiretap channel. To derive the maximum likelihood estimation method for the mean and variance, we first need the joint probability density function of the received samples at receiver.

1.2 Contributions

Based on the aforementioned literature, it can be easily inferred that the secrecy analysis of the diffusion-based molecular communication is a matter of grave concern and challenge. Thus the area of secure communication in the molecular communication paradigm is open and require a large amount of work. For this, the physical layer security would behave as an apt candidate for achieving secure communication between the transmitter and the receiver. Thus, an attempt has been made to evaluate the secrecy performance of the diffusion-based molecular timing channels by calculating the upper bound of average eavesdropper capacity and the secrecy metrics when the availability of the distance of the eavesdropper is assumed to be uniform, and Gaussian distributed random variable. The significant contributions of this manuscript are as follows:

- We have obtained the closed-form expressions of the upper bound of average capacity of the eavesdropper channel when the distance between transmitter and eavesdropper is assumed to be uniform, and Gaussian distributed.
- We have obtained approximate analytical expression for the upper bound on the eavesdropper channel capacity.
- The analytical expression for generalised secrecy outage probability is obtained when the distance of eavesdropper is assumed to be randomly distributed as uniform and Gaussian. Useful insights like secrecy diversity gain and secrecy diversity order are further drawn from the expression of generalised secrecy outage probability.
- Closed-form expression for average fractional equivocation of the system is calculated when the distance between transmitter and eavesdropper is assumed to be uniform and Gaussian distributed. It will provide the indication about the decoding error probability of confidential message in eavesdropper.
• The expression for the average information leakage rate to the eavesdropper is derived when the distance between transmitter and eavesdropper is assumed to be uniform and Gaussian distributed. This metric gives useful insights about how much and at what rate the confidential information is leaked to the eavesdropper.

The rest of the manuscript is organised as follows. Section 2 outlines the system model. Section 3 provides information-theoretic capacity analysis where upper bound of average eavesdropper capacity is calculated. Section 4 underlines the secrecy performance analysis for both uniform as well as Gaussian distribution regimes. Numerical results which evaluate the system’s performance are highlighted in Section 5, and finally, Section 6 concludes the manuscript.

Notation: The following notations would be used throughout the script: \( N(\mu, \sigma^2) \) represents Gaussian distributed random variable (r.v) with mean \( \mu \) and variance \( \sigma^2 \) meanwhile, \( U(a, b) \) is the uniformly distributed random variable (r.v) with duration from \( a \) to \( b \). \( \ln(\cdot) \), \( \text{erf}(\cdot) \) and \( \text{Ei}(\cdot) \) and \( Q(\cdot) \) functions represents the logarithmic, error, exponential integral and Q functions, respectively. The modified Bessel’s function is represented as \( I_0(\cdot) \). \( C_E \) represents the upper bound of average eavesdropper capacity. \( H(\cdot) \) denotes the entropy of the signal and \( H(\cdot|Y) \) is equivocation which represents the entropy of \( X \) conditioned to the observation signal \( Y \) at the destination. \( \mathbb{P}(\cdot) \) denotes the probability. Expectation operator is denoted by \( \mathbb{E}(\cdot) \).

## 2 SYSTEM MODEL

The system model for the diffusion-based molecular communication embodies a transmitting point unit, receiving unit and the channel (propagation) media. The whole of the system model comprises a transmitting point source, an aqueous environment and a destination capable of receiving the molecules, the block diagram of which is depicted in Figure 1. The transmitting point source enclosed within the physical system is proficiently transmitting the molecules of identical nature.

Similar to [6] the modulation of information, in this case, is considered to be in the time of release of molecules. Here, each particle is released in a particular time slot denoted by particle release time or transmit time \( T_t \). These released particles follow a random propagation path and are received at the receiver. The received particle arrives at a particular instant of time known to be the time of arrival which is denoted as \( T_a \). The time taken by the particles from the transmitter to receiver is known as the propagation delay and is denoted by \( T_p \). Mathematically, the time of arrival at the receiver is expressed as:

\[
T_a = T_t + T_p.
\]

The propagation delay \( (T_p) \) for the drift free scenario can be modeled as \( \alpha \)-stable Lévy distributed random variable \((\text{Lévy}(\mu, \epsilon))\) [25]. Mathematically, Lévy distributed random variable \((R)\) can be represented as:

\[
f_{R}(r; \mu, \epsilon) = \sqrt{\frac{\epsilon}{2\pi(r - \mu)^3}} \exp\left(\frac{-\epsilon}{2(r - \mu)}\right).
\]

where \( \mu \) is location parameter and \( \epsilon \) is scale parameter. The propagation delay time \( (T_p) \) is basically the additive noise term which can be written as \( T_p \sim \text{Lévy}(0, d^2/(2D)) \) and mathematically expressed as [6]:

\[
f_{T_p}(t_a) = \frac{d}{\sqrt{4\pi D t_n^{3/2}}} \exp\left(\frac{-d^2}{4D(t_a)}\right).
\]

The rate at which these molecules die-out is determined by the degradation parameter denoted as \( \alpha \), mathematically which is modeled as [6]:

\[
b(\tau) = \alpha \epsilon^{-\alpha \tau}, \quad \tau > 0,
\]

where \( \alpha \) is the degradation parameter and \( \tau \) is the lifetime of the molecules and \( b(\tau) \) is the exponentially decaying lifetime rate. Since in the scenario of molecular communication simultaneously large number of random processes are going on, thus it is optimum to assume that the transmitted molecules have a finite lifetime.

Moreover, the transmission of molecules from the point source transmitter to the destination receiver starts at \( t = 0 \) instant and at \( x = 0 \) position. The broadcasting of molecules into the aqueous media is proficiently done when the external parameters such as: temperature, viscosity and the flow of the media, remain same for all instants of time and distance. Molecules injected into the aqueous media traverse along the channel and are received by the destination unit. These molecules are then decoded and processed for further information. Furthermore, the modulation information is in the time of the release of molecules which is modeled as a truncated Lévy
distributed random variable \( (t_d) \) [6], which mathematically is represented as:

\[
f_{t_d} = \begin{cases} 0, & \text{for } t_d \leq 0 \\ \sqrt{\frac{d^2}{4\pi t_d}} e^{-\frac{d^2}{4t_d}} e^{-\frac{3}{2}(t_d)}, & \text{for } t_d > 0, \end{cases}
\]  

(5)

where \( e \) denote the noise parameter of Lévy distribution and \( d \) is the distance between transmitter and receiver.

The system model is based on the following assumptions:

- The system model is considered in the cartesian coordinate where the transmitting source is a point source. The transmitter block is broadcasting information molecules continuously.
- The propagation channel is free from the drift phenomenon, that is, the molecular motion is primarily governed by the random motion in the diffusion process. The channel media is having a well-defined Diffusion coefficient \( (D) \) which is dependent on the viscosity \( \eta \) and the temperature \( (T) \) of the aqueous media.
- The legitimate receiver is absorbing in nature and is located at a given position \( d_M \) from the transmitter.

Following the basic assumptions, the system model also lay the groundwork for determining the capacity bounds (both upper \( C_{ub} \) and lower \( C_{lb} \) bounds) on the channel. Based on the capacity bounds, the mathematical relationship between the eavesdropper capacity, the generalised secrecy outage probability, average fractional equivocation and average information leakage rate are what that leads to the fundamental theory of any secure communication.

3 | CAPACITY ANALYSIS

The mathematical expression which officially depicts the liaison between the information entropy \( (H(X) \) and \( H(X/Y) \)), the mutual information \( (I(X;Y)) \) and the capacity \( (C) \) of the channel is represented as:

\[
C = \max_{f_X(\cdot)} I(X : Y) = \max_{f_X(\cdot)} H(X) - H(X/Y),
\]

(6)

where \( I(X : Y) = I(T_i; T_o) \) that is the mutual information maximisation is based in terms of the transmit time \( (T_i) \) and the receiving or arrival time \( (T_o) \).

This, preliminary emanate from the fact that the capacity of the channel is defined as the maximum of the difference between the entropy of the main signal X and the conditional entropy of the main signal X provided the signal Y is observed. Thus, the upper bound on the capacity of diffusion-based molecular communication is given by [6] whose mathematical portrayal is represented as:

\[
C_{ub} \leq \ln\left(\left(\tau_m + \frac{e^{-\rho}}{p} e^{-\frac{\tau_m}{p}}\right)\right) + \frac{3}{2} \sqrt{\frac{p}{2\pi}} I_{1/2}(p)\ln\left(\frac{p}{e}\right)
\]

\[ -\frac{e^{-\rho}}{2} \left(1 + 2\rho - \ln\left(\frac{e}{2\pi}\right) - \frac{1}{\pi} (e^{2\rho} Ei(-2\rho) - Ei(2\rho))\right),\]

(7)

where

\[
\tau_m \gg \tau_x + E(T_u),
\]

(8)

and expectation obtained from [6] is represented as

\[
E(T_u) = e^{-\rho}\left(\sqrt{\frac{e}{2\pi}}\right).
\]

(9)

- \( \rho \) is termed as the noise parameter and is given by \( \rho = \frac{d^2}{2D} \)
- \( D \) = diffusion coefficient.
- \( \alpha \) is the degradation parameter.
- \( p \) is the scaled version of the noise parameter having value \( p = \sqrt{2\pi e} = (d\sqrt{\alpha/D}) \) where \( d \) is distance travelled by information molecules from source to destination.
- \( \tau_m \) is the average waiting time between the consecutive transmission of molecules and \( \tau_x \) is the symbol interval.
- \( I_{1/2}(p) \) denotes the modified Bessel’s function.
- \( Ei(\cdot) \) is the exponential integral represented as \( Ei(x) = \int_{-\infty}^{x} (e^z)/z \, dz \).

As the upper bound of the channel depicts the maximum capacity up to which the molecules can be transmitted from the transmitter to the receiver; thus the equality sign can be assumed for Equation (7). According to Figure 2, let us consider the scenario of eavesdropper in the system wherein the eavesdropper is denoted by Eve, the main transmitter as Alice and the main receiver as Bob. From the basics of information-theoretical security concepts, the amount of information that is leaked towards the eavesdropper during an ongoing legitimate communication is determined by the secrecy capacity \( (C_i) \). Since the mutual information between the legitimate receiver Bob is given by \( I(X;Y) \). But, in the case of information-stealing scenario, the leakage information is given as [11]:

\[
I(X;Z) = H(X) - H(X/Z),
\]

(10)

where \( Z \) is the signal received in eavesdropper (Eve). Moreover, the random motion of the particles increases the vulnerability of the molecules to be received at Eve rather than Bob. According to Figure 2, we have assumed that Bob is present at a fixed distance with respect to the transmitter. Simultaneously, the uncertainty in the distance of eavesdropper is discussed in the succeeding sections, wherein the eavesdropper distance is assumed to be uniform as well as Gaussian distributed.
3.1 Upper bound of average eavesdropper capacity when \( d_E \) is uniform distributed

Since there is no absolute prior knowledge of the distance \( (d_E) \) of the eavesdropper from the transmitter, but one can estimate it from its distribution statistics. Therefore, the eavesdropper distance is distributed like a uniform distributed random variable \( U(0, d_E) \) having a certain probability density function (p.d.f). Now, using the upper bound given by (7) the upper bound of average eavesdropper capacity can be calculated by,

\[
C_E = \int_0^{d_E} f_d(d) C_{ab} \, dx.
\]

On substituting (7) into (11) and using the p.d.f of uniform distribution we get:

\[
C_E = \int_0^{d_E} \frac{1}{d_E} \left[ \ln\left( \left( \tau_m + \frac{c}{\bar{p}} e^{-\bar{p}} \right) e \right) + \frac{3}{2} \sqrt{\frac{\bar{p}}{2\pi}} I_1(\bar{p}) \ln\left( \sqrt{\frac{\bar{p}}{\tau_m}} \right) \\
- \frac{e^{-\bar{p}}}{2} \left( 1 + 2\bar{p} - \ln\left( \frac{\bar{p}}{2\pi} \right) - \frac{1}{\bar{p}} (\gamma \bar{p} Ei(-2\bar{p}) - Ei(2\bar{p})) \right) \right] \, dx.
\]

Moreover, the distance of eavesdropper is a random variable and parameter \( \bar{p} \) is dependent on distance by the expression \( \bar{p} = d \sqrt{\frac{\tau_m}{\alpha}} \). Thus, the transformation of distance \( (d_E) \) r.v to performance parameter \( (\bar{p}) \) r.v yields the p.d.f of \( \bar{p} \) which is represented as:

\[
f_{\bar{p}}(\bar{p}) = \left\{ \begin{array}{ll}
\frac{1}{d_E} \left( \sqrt{\frac{\alpha}{D}} \right) & \text{for } 0 \leq \bar{p} \leq d_E \left( \sqrt{\frac{\alpha}{D}} \right).
\end{array} \right.
\]

In order to obtain a closed form solution of (12) we bifurcate the upper bound of average eavesdropper capacity equation into three integrals of \( I_{E1}, I_{E2} \) and \( I_{E3} \). These three integral values in mathematical relationship with eavesdropper capacity is represented as:

\[
C_E = I_{E1} + I_{E2} + I_{E3},
\]

where,

\[
I_{E1} = \int_0^{d_E} \frac{1}{d_E} \ln\left( \left( \tau_m + \frac{c}{\bar{p}} e^{-\bar{p}} \right) e \right) \, dx. \tag{15}
\]

Thus, the closed form solution of the above integral is mathematically represented as:

\[
I_{E1} = d_E \ln(\tau_m) + d_E + \frac{d_E^2}{2} - \frac{d_E^2}{2} \sqrt{\frac{\alpha}{D}} \\
+ \sum_{n \geq 2} \left( (\frac{1}{\alpha})^{n+1} (\gamma(n + 1, n d_E)) \right). \tag{16}
\]

where \( \gamma(n + 1, n d_E) \) is the lower incomplete gamma function. From (16), it can be observed that \( I_{E1} \) is the average capacity component of Eve link which is a function of \( \tau_m \). On the similar grounds, the mathematical representation of the integral \( I_{E2} \) is given as:

\[
I_{E2} = \left( \frac{3}{2\sqrt{2\pi}} \right) \left( \frac{D}{d_E \alpha} \right) \int_0^{p_1} \frac{\bar{p}^2}{\sqrt{2\pi}} I_{1/2}(\bar{p}) \left( \ln(2\alpha) - \ln(\bar{p}) \right) d\bar{p}, \tag{17}
\]

where \( p_1 = d_E \sqrt{\frac{\alpha}{D}} \). Thus by using integral by parts and the various identities of modified Bessel’s function \( (I_{1/2}(\bar{p})) \) the closed form solution is depicted as:

\[
I_{E2} = \left( \frac{3}{2\sqrt{2\pi}} \right) \left( \frac{D}{d_E \alpha} \right) \left[ \sqrt{p_1} L_{-1/2}(p_1) \ln(2\alpha) \right. \\
- p_1^{3/2} I_{1/2}(p_1) \ln(p_1) + p_1^{3/2} I_{1/2}(p_1) \\
- \ln(p_1) p_1^{3/2} I_{1/2}(p_1) - \frac{(\gamma^2 - 1)}{\sqrt{2\pi}} \\
\left. - \frac{2}{\pi} \left( \log(p_1) \right) p_1^{3/2} K_{-3/2}(p_1) + \sqrt{\frac{2}{\pi}} (1 - \bar{p}) \right]. \tag{18}
\]

where, \( L_{-1/2}, I_{1/2}, K_{-3/2} \) are the mathematical notation for modified Bessel’s functions, respectively. From (18) it can be observed that \( I_{E2} \) is a function of system parameters such as \( \alpha \) and \( D \). Moreover, \( I_{E2} \) being average capacity component of Eve link is independent of \( \tau_m \).
Lastly, the mathematical expression for the third integral \( I_{E3} \) as given in (14) is illustrated as:

\[
I_{E3} = -\frac{1}{d_E} \int_0^{d_E} e^{-d_E} \left( 1 + 2p - \ln \left( \frac{e}{2\pi} \right) \right) \ \mathrm{d}x
- \frac{1}{\pi} \left( e^{2p} Ei(-2p) - Ei(2p) \right) \ \mathrm{d}x,
\tag{19}
\]

where, \( p = d_E \sqrt{\alpha} \). In order to obtain the closed form expression of the above integral, we bifurcate these integrals into smaller individual parts. The solution of these individual integrals requires the integral identities of exponential integrals \( Ei(z) \). Thus the closed form expression of (19) is obtained as under:

\[
I_{E3} = -\frac{1}{d_E} \left[ \sqrt{D} \left( 1 - e^{-d_E} \sqrt{\frac{\pi}{\alpha}} \right) + d_E e^{-d_E} + e^{-d_E} - 1 \right.
+ \left( \ln(d_E) \frac{e^{-d_E} \sqrt{\frac{\pi}{\alpha}}}{\sqrt{\frac{\pi}{D}}} \right) - Ei \left( -d_E \sqrt{\frac{\alpha}{D}} \right)
+ \left( \ln(4\pi D) \frac{1 - e^{-d_E} \sqrt{\frac{\pi}{\alpha}}}{\sqrt{\frac{\pi}{D}}} \right)
- \sqrt{\frac{D}{\alpha}} \left( e^{d_E} \sqrt{\frac{\pi}{\alpha}} Ei \left( -2d_E \sqrt{\frac{\alpha}{D}} \right) - Ei \left( -d_E \sqrt{\frac{\alpha}{D}} \right) \right)
- \sqrt{\frac{D}{\alpha}} \left( e^{-d_E} \sqrt{\frac{\pi}{\alpha}} Ei \left( 2d_E \sqrt{\frac{\alpha}{D}} \right) - Ei \left( d_E \sqrt{\frac{\alpha}{D}} \right) \right) \right].
\tag{20}
\]

Substituting (16), (18) and (20) into (14) we get the upper bound of average eavesdropper capacity when the distance of the eavesdropper is uniformly distributed. Thus from the closed-form expression, it is important to note that the upper bound of the average eavesdropper is a function of physical parameters of the channels such as degradation parameter (\( \alpha \)), diffusion coefficient (\( D \) and \( \tau_\alpha \). From the expression it can be said that changing any of the above stated physical parameters causes a significant change on the upper bound of average eavesdropper capacity, which in-turn causes alterations in the system’s performance. Moreover, \( I_{E1} \) component shows the dependence of upper bound of average eavesdropper capacity on the average wait time between successive transmissions whereas \( I_{E2} \) and \( I_{E3} \) components show the dependence of upper bound of average eavesdropper capacity on the scaled version of Lévy noise parameter (\( \rho \)).

### 3.2 Upper bound of average eavesdropper capacity when \( d_E \) is Gaussian distributed

In contrast to the analysis undertaken in the previous section, this section constitutes the scenario, when the eavesdropper distance is Gaussian distributed \( d_E \sim \mathcal{N}(\mu_x, \sigma_x^2) \), where \( \mu_x \) is the mean and \( \sigma_x^2 = \sigma_E^2 \) is the variance of the eavesdropper distance. Now, to determine the upper bound of average eavesdropper capacity, we have to integrate the capacity over the interval 0 to \( d_E \). Mathematically, the eavesdropper capacity is given as:

\[
C_E = \int_0^{d_E} f_\alpha(x) C_{eb} \, dx.
\tag{21}
\]

Additionally, the relationship of distance \( d_E \) with the performance parameter (\( p \)) is given by the expression \( p = d(\sqrt{\alpha} / D) \). Thus the transformation of the Gaussian distributed random variable \( d_E \) into another Gaussian distributed random variable \( p \) yields new p.d.f of this new random variable which is illustrated as:

\[
f_p(p) = \frac{1}{\sqrt{2\pi \sigma_p^2}} e^{-\frac{(x-\mu_p)^2}{2\sigma_p^2}},
\tag{22}
\]

where \( \mu_p \) is the mean of this new random variable having value \( \mu_p = \sqrt{\frac{\alpha}{D}} \mu_x \) and \( \sigma_p^2 \) is the variance of the \( p \) random variable with \( \sigma_p^2 = \frac{\alpha}{D} \sigma_x^2 \). Therefore, by substituting (7) into (21) we are able to obtain the eavesdropper capacity expression.

\[
C_E = \int_0^{d_E} \left( \frac{1}{\sqrt{2\pi \sigma_x^2}} e^{-\frac{(x-\mu_x)^2}{2\sigma_x^2}} \right) \ln \left( \left( \tau_\alpha + \frac{e}{p} e^{-p} \right) e \right)
+ 3 \frac{\sqrt{\frac{\alpha}{D}}}{2\pi} I_{I2}(p) \ln \left( \frac{p}{\tau_\alpha} \right)
- \frac{e^{-\frac{\mu_x}{p}}}{2} \left( 1 + 2p - \ln \left( \frac{e}{2\pi} \right) - 1 \frac{e^2 Ei(-2p) - Ei(2p)}{} \right) \ \mathrm{d}x.
\tag{23}
\]

Again for obtaining the closed-form solution of the above complicated definite integral, we need to bifurcate this integral expression into smaller individual integrals. Thus, the modified expression of eavesdropper capacity, as indicated in (23) is obtained as:

\[
C_E = I_{E1} + I_{E2} + I_{E3},
\tag{24}
\]

where

\[
I_{E1} = \int_0^{d_E} \left( \frac{1}{\sqrt{2\pi \sigma_x^2}} e^{-\frac{(x-\mu_x)^2}{2\sigma_x^2}} \right) \ln \left( \left( \tau_\alpha + \frac{e}{p} e^{-p} \right) e \right) \ \mathrm{d}x.
\tag{25}
\]
The closed-form expression of (25) is obtained in (26), which is given as

\[ I_{F_1} = \frac{1}{2\sqrt{2\sigma_p^2}} F_1 \ln(\tau_w) + F_2 + F_3 + F_4 + F_5 \]

\[ + \frac{\sqrt{2\sigma_p^2}}{2\alpha \tau_w} \left[ F_6 + F_7 + \frac{\mu_p}{\sqrt{2\sigma_p^2}} \right] \]

\[ - \frac{\sqrt{2\sigma_p^2}}{2\alpha \tau_w} \left[ F_8 + F_9 + F_{10} + \frac{\mu_p}{\sqrt{2\sigma_p^2}} \right], \quad (26) \]

where

\[ F_1 = \frac{1}{\sqrt{a_{11}}} e^{\left( \frac{\sqrt{2\sigma_p^2}}{a_{11}} \right)} \text{erf} \left( p_1 \sqrt{a_{11}} + \frac{b_{11}}{\sqrt{a_{11}}} \right) \]

\[ - \frac{1}{\sqrt{a_{11}}} e^{\left( \frac{\sqrt{2\sigma_p^2}}{a_{11}} \right)} \text{erf} \left( \frac{b_{11}}{\sqrt{a_{11}}} \right), \quad (27) \]

\[ F_2 = \frac{1}{\sqrt{a_{12}}} e^{\left( \frac{\sqrt{2\sigma_p^2}}{a_{12}} \right)} \text{erf} \left( p_1 \sqrt{a_{12}} + \frac{b_{12}}{\sqrt{a_{12}}} \right) \]

\[ - \frac{1}{\sqrt{a_{12}}} e^{\left( \frac{\sqrt{2\sigma_p^2}}{a_{12}} \right)} \text{erf} \left( \frac{b_{12}}{\sqrt{a_{12}}} \right), \quad (28) \]

\[ F_3 = \frac{2}{a_{13}} \ln \left( 1 + \frac{p_1 e^{-\mu_p}}{2\alpha \tau_w} \right) e^{\left( \frac{\sqrt{2\sigma_p^2}}{a_{13}} \right)} \]

\[ \text{erf} \left( p_1 \sqrt{a_{13}} + \frac{b_{13}}{\sqrt{a_{13}}} \right), \quad (29) \]

\[ F_4 = e^{-\mu_p} \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \text{erf} \left( \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right), \quad (30) \]

\[ F_5 = \frac{e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)}}{2\alpha \tau_w} \text{erf} \left( -\frac{\sqrt{\sigma_p^2}}{2} - \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right), \quad (31) \]

\[ F_6 = -\frac{e^{-\mu_p}}{2\alpha \tau_w} \text{erf} \left( \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \left( \frac{p_1 - \mu_p + 1}{\sqrt{2\sigma_p^2}} \right) \right), \quad (32) \]

\[ F_7 = e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)} \frac{1}{\sqrt{2\sigma_p^2}} \text{erf} \left( \frac{\sigma_p^2}{\sqrt{2\sigma_p^2}} \right) \]

\[ \left( \frac{\sigma_p^2}{2} - \mu_p \right) \frac{1}{\sqrt{2\sigma_p^2}} \text{erf} \left( \frac{\sigma_p^2}{\sqrt{2\sigma_p^2}} \right), \quad (33) \]

\[ F_8 = -e^{-\mu_p} \text{erf} \left( \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right) \]

\[ + e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)} \text{erf} \left( -\frac{\sigma_p^2}{2} - \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right), \quad (34) \]

\[ F_9 = -\frac{1}{2\alpha \tau_w} \text{erf} \left( \frac{\sigma_p^2}{\sqrt{2\sigma_p^2}} \right) \]

\[ - e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)} \text{erf} \left( -\frac{\sigma_p^2}{2} - \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right), \quad (35) \]

\[ F_{10} = e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)} \frac{1}{\sqrt{2\sigma_p^2}} \text{erf} \left( -\frac{\sigma_p^2}{2} - \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right) \]

\[ - e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)} \frac{1}{\sqrt{2\sigma_p^2}} \text{erf} \left( -\frac{\sigma_p^2}{2} - \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right), \quad (36) \]

\[ F_{11} = -\text{erf} \left( \frac{-\sigma_p^2}{\sqrt{2\sigma_p^2}} \right) + e^{\left( \frac{\sqrt{2\sigma_p^2}}{2} - \mu_p \right)} \text{erf} \left( -\frac{\sigma_p^2}{2} - \frac{p_1 - \mu_p}{\sqrt{2\sigma_p^2}} \right), \quad (37) \]

Here, \( p_1 = \left( d_E \sqrt{\frac{\sigma_p^2}{2}} \right), a_{11} = a_{12} = a_{13} = \left( \frac{1}{2\alpha \tau_w} \right), b_{11} = b_{12} = \]

\( b_{13} = \left( \frac{-\mu_p}{2\sigma_p^2} \right), \quad \alpha_1 = \alpha_2 = \alpha_3 = \left( \frac{\mu_p^2}{2\sigma_p^2} \right). \) From (26) it can be noted that the average Eve capacity component \( (I_{E_1}) \) is a function of \( \tau_w, \alpha, \text{mean of eavesdropper distance} (\mu_p), \) and variance \( (\sigma_p^2). \) Since \( I_{E_1} \) is a function of variance thus it can be observed from mathematical expression that with increasing variance the average eavesdropper capacity component decreases.
Likewise, the mathematical expression for the integral $I_{E_2}$ present in (24) is given as:

\[
I_{E_2} = \frac{3}{2} \int_0^{\beta_1} \sqrt{\frac{p}{2\pi}} I_{1/2}(p) \ln \left( \frac{2\pi}{p} \right) \left( \frac{1}{\sqrt{2\pi \sigma^2_p}} \right) \left( e^{\frac{(p-\mu_p)^2}{2\sigma^2_p}} \right) dp,
\]

(38)

In (38) the term $I_{1/2}(p)$ is the modified Bessel’s function which can be replaced by its equivalent hyperbolic function. The equivalent expression for modified Bessel’s function is represented as:

\[
I_{1/2}(p) = \sqrt{\frac{2}{\pi}} \sinh \left( \frac{p}{\sqrt{p}} \right).
\]

(39)

Now by substituting (39) in (38) and using integral by parts identities, we are now in a position to compute the closed form expression of integral $I_{E_2}$. Therefore, the closed-form expression is written as:

\[
I_{E_2} = \frac{3\ln(2\pi)}{\sqrt{\sigma^2_p}} \left\{ \sigma_p \sinh(\tau_1) \text{erf}(\tau_1) + \frac{(\sigma_p)^2}{2\sqrt{2\sigma^2_p}} e^{\frac{\sigma^2_p}{2}} \text{erf}(\tau_0) + \frac{e^\sigma \sqrt{2\sigma^2_p}}{2\sqrt{2\sigma^2_p}} e^{t_2} \right\}
\]

(40)

where $\tau_1 = \frac{\ln(2\pi)}{\sqrt{\sigma^2_p}}$ and $\tau_0 = \frac{-\mu_p}{\sqrt{\sigma^2_p}}$ respectively. From (40) it can be observed that the average Eve capacity component ($I_{E_2}$) is a function of $\alpha$, scaled version of Lévy noise parameter (p), $\mu_x$ and $\sigma^2_E$. Since $I_{E_2}$ is a function of variance thus it can be observed from mathematical expression that with increasing variance the average eavesdropper capacity component decreases. Finally, after obtaining the closed-form expression of the integral $I_{E_2}$ only the solution of integral $I_{E_3}$ is left whose mathematical expression is given by:

\[
I_{E_3} = \frac{1}{\sqrt{2\pi \sigma^2_p}} \int_0^{\beta_1} \left( 1 + 2p - \ln \left( \frac{e}{2\pi} \right) - \frac{(p-\mu_p)^2}{2\sigma^2_p} \right) dp,
\]

(41)

where $p$ and $e$ have the usual meaning. The closed-form expression is obtained as:

\[
I_{E_3} = \left[ \frac{(\sigma^2_p - \mu_p)}{4} \right] \left\{ \text{erf} \left( \tau_1 + \sqrt{\frac{\sigma^2_p}{2}} \right) - \text{erf} \left( \tau_0 + \sqrt{\frac{\sigma^2_p}{2}} \right) \right\}
\]

(42)

where $\tau_1 = \frac{\ln(2\pi)}{\sqrt{\sigma^2_p}}$ and $\tau_0 = \frac{-\mu_p}{\sqrt{\sigma^2_p}}$, respectively. Thus after obtaining the closed-form expression for the integrals $I_{E_1}, I_{E_2}$ and $I_{E_3}$, we now substitute (26), (40) and (42) in (24) so as to obtain the upper bound of eavesdropper capacity for Gaussian distributed random variable. Similar to the expression of the upper bound of average eavesdropper capacity obtained when $d_E$ is uniform distribution, the above expression of average eavesdropper capacity is also a function of physical parameters of the channel such as degradation parameter ($\alpha$), diffusion coefficient ($D$), mean of eavesdropper distance ($\mu_x$), variance ($\sigma^2_E$) etc. Also, $I_{E_3}$ component of (24) shows the dependence of the upper bound of average eavesdropper capacity on the average wait time between successive transmissions whereas $I_{E_2}$ and $I_{E_3}$ components shows the dependence of upper bound of average eavesdropper capacity on the scaled version of Lévy noise parameter (p).
Shannon’s definition for perfect secrecy along with strong and weak secrecy all belong to the classical secrecy approach. Since classical secrecy is not achievable in real-time scenarios, thus it is not convenient to use these metrics for practical analysis. Also, the classical approach doesn’t give any insight about eavesdropper decodability and average information leakage. Thus it becomes more imperative to use more robust and generalised secrecy metrics which finds perfect analogy with the real-world challenges. The subsequent section highlights the scenario of secrecy metrics in the case when the perfect secrecy is not achievable.

4 | SECRECY PERFORMANCE ANALYSIS

Consider the basic wiretap channel, as shown in Figure 2. From the figure, it can be easily said that instantaneous CSI (channel state information) of the Eve is not available at Alice. Thus, conventional secrecy outage probability is employed for measuring the secrecy performance of the system. But conventional secrecy outage probability has a strong condition on Eve’s decoding error probability, that is, $\delta \rightarrow 1$. Meanwhile, the conventional secrecy analysis fails when Eve’s decoding error probability $\delta$ ranges from 0 to 1, that is, $0 < \delta \leq 1$. Thus instead of conventional secrecy outage probability, we now use three secrecy metrics: generalised secrecy outage probability ($P_{out}$), average fractional equivocation, and average information leakage ($R_{e}$).

The term equivocation is used for quantifying the scenario of partial secrecy. This basically gives the information about the confusion level of eavesdropper. The fractional equivocation ($\Delta$) as defined in [26, 27] mathematically is represented as:

$$\Delta = \frac{H(X|Z)}{H(X)}.$$  (43)

For the wireless scenario the fractional equivocation is given in [26, Equation 7] where $C_M$, $C_t$ were main channel and eavesdropper capacities and $R$ was the secrecy rate. In [26] the signal to noise ratio (SNR) of both Bob and Eve were considered to be exponential distributed. But in molecular communication particularly in our system model we have taken the distance of eavesdropper to be uniform and Gaussian distributed while fixing the main channel distance. Thus the mathematical representation of fractional equivocation in terms of eavesdropper capacity considered in [26] was obtained as:

$$\Delta = \begin{cases} 1, & \text{for } C_E \leq C_M - R_t, \\ \frac{C_M - C_E}{R_t}, & \text{for } C_M - R_t < C_E < C_M, \\ 0, & \text{for } C_M \leq C_E, \end{cases}$$  (44)

where $\Delta$ = fractional equivocation. Notice that these three conditions for $\Delta$ represent different levels of confusion at Eve. First, when $C_E \leq C_M - R_t$, the equivocation $\Delta = 1$ indicates that no information leaks to Eve and she can just randomly guess about the transmitted message. The opposite condition yielding $\Delta = 0$, that is associated with $C_M \leq C_E$, implies that secure communication is not possible. Finally, the intermediate case when $\Delta = \frac{C_M - C_E}{R_t}$ represents a partial secrecy regime, in which only a fraction of the communication is secure. Unlike the conventional equivocation as explained in [28, Equation 2], the fractional equivocation as given by (43) depends on the channel only and is independent of the source. Since, eavesdropper capacity can be approximated as a function of distance (proof in appendix) is given by,

$$C_E \approx 1 + \ln(d_{E}) - \ln(\sqrt{4Dr_e}).$$  (45)

The fractional equivocation as given by (44) can be modified in terms of eavesdropper distance as:

$$\Delta = \begin{cases} 1, & \text{for } d_{E} \leq e^{R_t - R_e - A} \\ \frac{R_t - \ln(d_{E}) - A}{R_t}, & \text{for } e^{R_t - R_e - A} < d_{E} < e^{R_e - A} \\ 0, & \text{for } e^{R_e - A} \leq d_{E}, \end{cases}$$  (46)

where $A = 1 - \ln(\sqrt{4Dr_e})$ and $R_e \leq C_M$. The following subsections show the detailed analysis of three metrics (generalised secrecy outage probability, average fractional equivocation and average information leakage rate) which would be used to evaluate the secrecy performance of the molecular channel when eavesdropper distance is uniform as well as Gaussian distributed.

4.0.1 | Generalised secrecy outage probability

The generalised secrecy outage probability represents the probability that the ratio of information leakage is larger than a certain value. Mathematically, generalised secrecy outage probability is represented as:

$$P_{out} = P(\Delta < \phi),$$  (47)

where $P(\cdot)$ is the probability function of an event and $\phi$ is the minimum value of fractional equivocation whose value varies from 0 to 1 ($0 < \phi \leq 1$). Note that the usual formulation for the secrecy outage probability only considers $C_E \leq C_M - R_t$, which corresponds to case when $\phi = 1$. Since the fractional equivocation denotes the decoding error probability of the eavesdropper, thus generalised secrecy outage probability is applicable for all practical scenarios. Moreover, the conventional secrecy outage probability is a special case of generalised secrecy outage probability metric. Using (46) the expression for generalised secrecy outage probability can be obtained as:

$$P_{out} = P(d_{E} \geq e^{R_t - R_e - A}) + P(e^{R_t - R_e - A} < d_{E} < e^{R_e - A})$$

$$\cdot P\left(\frac{R_t - \ln(d_{E}) - A}{R_t} < \phi \mid e^{R_t - R_e - A} < d_{E} < e^{R_e - A}\right).$$  (48)
4.0.2 Average fractional equivocation

The average fractional equivocation is defined as expectation of fractional equivocation. By taking expectation of (46) we can obtain the value of average fractional equivocation. Mathematically the average fractional expectation is given as

\[ \bar{\Delta} = \mathbb{E}(\Delta), \tag{49} \]

where \( \mathbb{E}(.) \) denotes the expectation operator. The average fractional equivocation gives the asymptotic lower bound on the decoding probability of eavesdropper.

4.0.3 Average information leakage rate

When there is a prerequisite knowledge about the secrecy rate \((R_s)\) of the system then the rate at which certain amount of information leaked to eavesdropper is defined as the average information leakage rate. This average information leakage rate is given as:

\[ R_L = \mathbb{E}\{ (1-\Delta)R_s \} = (1-\bar{\Delta})R_s, \tag{50} \]

here we have taken a fixed amount of secrecy rate \((R_s)\). The average information leakage rate signifies that how fast the information is leaked to the eavesdropper. Lastly, as the exact value of the distance of the eavesdropper is not known, thus the following sections show secrecy analysis for different case scenarios when the distance is uniform as well as Gaussian distributed.

4.1 Secrecy performance analysis when \( d_E \) is uniform distributed

In this section, we majorly focus on calculating the secrecy performance metric of the system when the eavesdropper distance is exhibiting a uniform distribution scenario. Based on (48) the expression for generalised secrecy outage probability when eavesdropper distance is uniform distributed is obtained as:

\[ P_{\text{out}} = \int_{\bar{\beta}}^{\beta} \frac{1}{d_E} \, d\xi + \int_{\bar{\beta_1}}^{\beta_1} \frac{1}{d_E} \, d\xi, \tag{51} \]

where \( \bar{\beta} = e^{R_b-R_s-\phi-A} \) and \( \beta = e^{R_b-A} \). Finally, by substituting \( \bar{\beta} \) and \( \beta_1 \) in (51) we obtain generalised secrecy outage probability as

\[ P_{\text{out}} = 1 - \frac{e^{R_b-R_s-\phi-A}}{d_E}, \tag{52} \]

where \( A = 1 - \ln(\sqrt{4D\xi}) \) and \( 0 < \phi \leq 1 \). In general, for any value of \( \phi, 0 < \phi \leq 1 \), the Taylor series expansion of (52), which gives generalised secrecy outage probability for \( R_b > R_s \), can be represented as:

\[ P_{\text{out}} = 1 - \frac{1}{\sqrt{12\varphi}} - \frac{(R_b - R_s - \phi - A)}{\sqrt{12\varphi}} - O(R_b - R_s - \phi - A), \tag{53} \]

where \( O(R_b - R_s - \phi - A) \) represents the other higher order terms. Now comparing (53) with

\[ P_{\text{out}}^\infty = (G_c, \sigma^2)^{-G_d} + O(\sigma^2)^{-G_d}, \tag{54} \]

we obtain the values of diversity gain \((G_d)\) and secrecy gain \((G_c)\) as

\[ G_d = \frac{1}{2}, \tag{55} \]

and

\[ G_c = \frac{\sqrt{12}}{A + R_s - R_b}. \tag{56} \]

Remarks. Based on \( G_d \) and \( G_c \), following observations can be made.

- Secrecy diversity order is found to be a constant value independent of other parameters like \( \alpha, D, d_M, d_E \) etc.
- Secrecy Gain increases with the increase in the main channel rate \( R_s \).
- For a higher value of \( \alpha \) and \( D \) the secrecy gain \( G_c \) improves.
- For higher values of rate \( R_s \), the secrecy gain degrades.
- Secrecy Gain is a function of fractional equivocation \( \phi \). \( G_c \) is inversely proportional to \( \phi \), that is, for \( \phi \) ranging from 0 to 1 the secrecy gain \( G_c \) degrades.

For \( \phi = 1 \), Equation (52) reduces to special case of classical secrecy outage probability which is given as:

\[ P_{\text{out}} = 1 - \frac{e^{R_b-R_s-A}}{d_E}. \tag{57} \]

Using Taylor series expansion in (57), and also substituting \( d_E = \sqrt{12\varphi^2} \), the outage probability for \( R_b > R_s \) can be represented as

\[ P_{\text{out}} = 1 - \frac{1}{\sqrt{12\varphi^2}} - \frac{(R_b - R_s - A)}{\sqrt{12\varphi^2}} - O(R_b - R_s - A), \tag{58} \]

where \( O(R_b - R_s - A) \) represents the other higher order terms. Now by comparing (58) with (54) we obtain the values of diversity gain \((G_d)\) and secrecy gain \((G_c)\) as

\[ G_d = \frac{1}{2}, \tag{59} \]

and

\[ G_c = \frac{\sqrt{12}}{A + R_s - R_b}. \tag{60} \]
Remark. Based on the comparative analysis between (56) and (60), it can be noted that for $\phi = 1$ the generalised secrecy outage probability becomes classical secrecy outage probability. Also as $\phi$ is changed from 1 to 0 the secrecy gain improves which can be observed from (56).

Furthermore, to calculate the average fractional equivocation for the case when eavesdropper distance is uniform distributed we use (49) which is basically the expectation of fractional equivocation obtained in (46). This is mathematically obtained as:

$$\Delta = \int_0^\lambda \frac{1}{d_E} \, dx + \int_\lambda^1 \frac{1}{d_E} \left( \frac{R_b - A}{R_s} \right) \left( \lambda_1 - \lambda \right) \, dx \tag{61}$$

where $\lambda = e^{R_s - R_s - A}$ and $\lambda_1 = \beta = e^{R_s - A}$. Thus average fractional equivocation is given by:

$$\Delta = \frac{\lambda}{d_E} + \left( \frac{R_s - A}{R_s d_E} \right) (\lambda_1 - \lambda)$$

$$- \left( \frac{\lambda_1 \ln(\lambda_1) - \lambda_1 - \lambda_1 \ln(\lambda) + \lambda}{R_s d_E} \right). \tag{62}$$

Simultaneously, the average information leakage rate ($R_L$) as obtained by (50) for the uniformly distributed eavesdropper distance is given as:

$$R_L = R_s \left( 1 - \frac{\lambda}{d_E} - \frac{R_b - A}{R_s d_E} (\lambda_1 - \lambda) \right)$$

$$+ \lambda \left( \frac{\lambda_1 \ln(\lambda_1) - \lambda_1 - \lambda_1 \ln(\lambda) + \lambda}{R_s d_E} \right). \tag{63}$$

### 4.2 Secrecy performance analysis when $d_E$ is Gaussian distributed

The primary focus of this section is to calculate the expressions for the various secrecy metrics (generalised secrecy outage probability, average fractional equivocation and average information leakage rate) when the eavesdropper distance is Gaussian distributed with mean $\mu_\gamma$ and variance $\sigma^2_\gamma$. Now using (48) the expression for generalised secrecy outage probability can be derived as:

$$P_{out} = \int_{\beta}^\infty \frac{1}{\sqrt{2\pi\sigma^2_\gamma}} \, e^{-\frac{(\gamma - \mu_\gamma)^2}{2\sigma^2_\gamma}} \, dx$$

$$+ \int_0^{\beta_1} \frac{1}{\sqrt{2\pi\sigma^2_\gamma}} \, e^{-\frac{(\gamma - \mu_\gamma)^2}{2\sigma^2_\gamma}} \, dx \tag{64}$$

where $\beta_1 = e^{R_s - R_s - A}$, $\beta = e^{R_s - A}$ and $A = 1 - \ln(\sqrt{4D\alpha})$. Similar to generalised secrecy outage probability in uniform distribution case we substitute $\beta$ and $\beta_1$ in (64) to obtain generalised secrecy outage probability which can be written as:

$$P_{out} = Q\left(\frac{\beta - \mu_\gamma}{\sqrt{\sigma^2_\gamma}}\right) + Q\left(\frac{\beta_1 - \mu_\gamma}{\sqrt{\sigma^2_\gamma}}\right) - Q\left(\frac{\beta - \mu_\gamma}{\sqrt{\sigma^2_\gamma}}\right). \tag{65}$$

Thus the above terms can be further reduced and an expression for generalised secrecy outage probability can be obtained as:

$$P_{out} = Q\left(\frac{e^{R_s - R_s - A} - \mu_\gamma}{\sqrt{\sigma^2_\gamma}}\right). \tag{66}$$

where $A = 1 - \ln(\sqrt{4D\alpha})$ and $0 < \phi \leq 1$. For any value of $\phi$ ($0 < \phi \leq 1$), the approximate expression for (66) can be obtained by using $Q$ function approximation as given in [29]. Mathematically, the approximate expression of generalised secrecy outage probability is obtained as:

$$P_{out} \approx 1 - \frac{1}{12} e^{-\frac{(\gamma - \mu_\gamma)^2}{2\sigma^2_\gamma}} - 4 e^{-\frac{(\gamma - \mu_\gamma)^2}{2\sigma^2_\gamma}} \tag{67}$$

where $\gamma = \frac{e^{R_s - R_s - A} - \mu_\gamma}{\sqrt{\sigma^2_\gamma}}$. By comparing (67) with

$$P_{out}^\infty = (G_{\sigma_\gamma^2}^2)^{-G_d} + O(\sigma_\gamma^2)^{-G_d}, \tag{68}$$

the value of the diversity gain $G_d$ can be obtained as:

$$G_d = 1, \tag{69}$$

and

$$G_c = \frac{24}{5(e^{R_s - R_s - A} - \mu_\gamma)^2}. \tag{70}$$

Remarks. Based on $G_d$ and $G_c$, following observations can be made.

- Secrecy diversity order is found to be unity, $G_d$ is independent of other parameters like $\alpha$, $D$, $d_M$, $d_E$, etc.
- Secrecy Gain is a function of fractional equivocation. As the fractional equivocation is increased from 0 to 1, the secrecy gain becomes worse.
- Secrecy gain increases with the increase in the main channel rate $R_s$.
- For a higher value of $\alpha$ and $D$ the secrecy gain $G_c$ improves.
- For higher values of rate $R_s$, the secrecy gain becomes worse.

When $\phi = 1$ the expression of generalised secrecy outage probability reduces to classical secrecy outage which is obtained...
as:

\[ P_{\text{out}} = \begin{cases} \frac{Q\left(\frac{\beta - \mu_x}{\sqrt{\sigma^2_x}}\right)}{\gamma_1} & \text{for } \mu_x \leq e^{\beta - \mu_x}, \\ 1 - Q\left(\frac{\beta - \mu_x}{\sqrt{\sigma^2_x}}\right) & \text{for } \mu_x > e^{\beta - \mu_x} \end{cases} \]

where \( \gamma_1 = e^{\beta - \mu_\lambda} \sqrt{\sigma^2_x} \). By comparing (72) and (68), the value of the diversity gain \( G_d \) and secrecy gain \( G_s \) can be obtained as:

\[ G_d = 1, \quad G_s = \frac{24}{5(e^{\beta - \mu_\lambda} - \mu_x)^2}. \]

**Remark.** Based on the comparative analysis between (70) and (74), it can be noted that for \( \phi = 1 \) the generalised secrecy outage probability becomes classical secrecy outage probability. Also as \( \phi \) is changed from 1 to 0 the secrecy gain improves which can be observed from (70).

Meanwhile, using (49) the expression for average fractional equivocation, which is expectation of fractional equivocation, can be calculated when the distance of eavesdropper is Gaussian distributed. Mathematically, the expression for average fractional equivocation is given by:

\[ \Delta = \int_0^\lambda \frac{1}{\sqrt{2\pi\sigma^2_x}} e^{-\frac{(\phi - \mu_\lambda)^2}{2\sigma^2_x}} \, d\phi \\
+ \int_\lambda^\lambda \frac{1}{\sqrt{2\pi\sigma^2_x}} e^{-\frac{(\phi - \mu_\lambda)^2}{2\sigma^2_x}} \left( \frac{R_b - \ln(x) - A}{R_b} \right) \, d\phi, \quad (75) \]

where \( \lambda = e^{R_b - \mu_\lambda} \) and \( \lambda_1 = \beta = e^{R_b - \mu_\lambda} \). Thus average fractional equivocation is given by:

\[ \Delta = 1 - Q\left(\frac{\lambda - \mu_\lambda}{\sqrt{\sigma^2_\lambda}}\right) + \left(\frac{R_b - A}{R_b}\right) \left\{ Q\left(\frac{\lambda_1 - \mu_\lambda}{\sqrt{\sigma^2_\lambda}}\right) - Q\left(\frac{\lambda - \mu_\lambda}{\sqrt{\sigma^2_\lambda}}\right) \right\}. \]

**5 | NUMERICAL ANALYSIS**

On the basis of the mathematical analysis undertaken in the preceding section the plots between average eavesdropper capacity (\( C_E \)), the generalised secrecy outage probability (\( P_{\text{out}} \)), the average fractional equivocation (\( \Delta \)) and the average information leakage rate (\( R_L \)) with respect to eavesdropper variance (\( \sigma^2_E \)) for uniform distribution scenario are obtained in Figures 3, Figure 4, Figure 5 and Figure 6, respectively. Simultaneously, the plots between average eavesdropper capacity (\( C_E \)), the generalised secrecy outage probability (\( P_{\text{out}} \)), the average fractional equivocation (\( \Delta \)) and the average information leakage rate (\( R_L \)) with respect to eavesdropper variance (\( \sigma^2_E \)) for Gaussian distribution scenario are shown Figure 7, Figure 8, Figure 9 and Figure 10, respectively.

Figure 3 depicts the variation of the upper bound of average eavesdropper capacity with respect to the variance for different values of degradation parameter in uniform distribution scenario. Here, the upper bound of average eavesdropper capacity decreases with a simultaneous increase in the variance of the eavesdropper distance (\( \sigma^2_E \)). This can be inferred from the fact that the increase in the variance values causes the increase in the entropy of the channel, which in-turn decreases capacity. Further, for higher values of variance, the plots tend to
**FIGURE 4** Generalised secrecy outage probability when the distance is uniform distributed r.v. Here secrecy rate \((R_s)\) is 0.1

**FIGURE 5** Average fractional equivocation when the distance is uniform distributed r.v.

**FIGURE 6** Average information leakage rate \((R_L)\) when the distance is uniform distributed r.v.

**FIGURE 7** Upper bound of average eavesdropper capacity when the distance is Gaussian distributed r.v.

**FIGURE 8** Generalised secrecy outage probability when the distance is Gaussian distributed r.v. Here secrecy rate \((R_s)\) is 0.1

**FIGURE 9** Average fractional equivocation when the distance is Gaussian distributed r.v.
Figure 10 presents the plot of average information leakage rate ($R_L$) when the distance is Gaussian distributed as a function of variance. The graph shows that as the variance increases, the average information leakage rate also increases. This indicates that the eavesdropper variance and the secrecy rate ($R_s$) are increased. Since $R_s$ practically informs the amount of confidential information leaked to the eavesdropper so for the higher value of variance $R_s$ approaches $R_c$. Meanwhile, increasing $\alpha$ causes $R_s$ to decrease while keeping secrecy rate $R_c$ to a particular value. This is mainly because increasing $\alpha$ causes the molecule to disintegrate rapidly, thereby causing the particle to be useless.

Figure 7 represents the plot of upper bound of average eavesdropper capacity as a function of eavesdropper variance ($\sigma^2$) for different values of degradation parameter ($\alpha$) when the distance is Gaussian distributed. Moreover, from the figure, it is evident that for increasing values of eavesdropper variance ($\sigma^2$), the upper bound of average eavesdropper capacity shows a decreasing trend. Note that similar to Figure 3, the upper bound of average eavesdropper capacity tends to converge for higher values of variance. However, for a given eavesdropper variance ($\sigma^2$), the upper bound of average eavesdropper capacity decreases as $\alpha$ is increased from 0.2 to 0.4.

The behaviour of generalised secrecy outage probability ($P_{out}$) with the increasing values of the eavesdropper variance ($\sigma^2$) for the Gaussian distribution regime, both by analytical and simulation method, is shown in the form of a plot as depicted in Figure 8. Note that for different degradation parameter ($\alpha$) values $\phi = 1$ represents the special case of classical secrecy outage probability. Moreover, from the figure, it can be analysed that by increasing the variance of eavesdropper distance ($\sigma^2$), the effect on the outage probability ($P_{out}$) is more prominent as the increasing variance causes rapid decay in the $P_{out}$ values. Also, the increase in values of $\alpha$ causes the outage probability to decrease; this is mainly because the increasing value of $\alpha$ causes the molecules to degrade rapidly. Hence, this rapid decay of transmitted molecules, causes less number of molecules to reach the eavesdropper, thereby decreasing generalised secrecy outage probability.

Simultaneously, the variation of average fractional equivocation ($\Delta$) with respect to increasing eavesdropper distance for different values of secrecy rate ($R_s$) in Gaussian distribution regime is plotted in Figure 9. From the figure, it can be visualised that $\Delta$ decreases simultaneously with respect to increasing variance as well as with increasing $R_s$. Moreover, even if $R_s$ becomes zero the average fractional equivocation ($\Delta$) is non-zero. Furthermore, simultaneous increase in the degradation parameter ($\alpha$) value causes a significant increase in $\Delta$. Thus, both channel parameters ($\alpha$ and $R_s$) play a vital role in controlling the secrecy performance of diffusive molecular communication systems.

Figure 10 represents the plot of average information leakage rate ($R_L$) as a function of eavesdropper variance for different values of $R_s$. It can be noted that the amount of information leaked to the eavesdropper, given by $R_L$, increases with increasing eavesdropper variance. The point which can also be noted that, for different $R_s$ values, the system has different secrecy outage probability.

The secrecy performance measured in terms of average information leakage rate ($R_L$) which is a function of the variance of eavesdropper distance, is illustrated in Figure 6. As shown in the figure, the average information leakage rate ($R_L$) increase as the eavesdropper variance and the secrecy rate ($R_s$) are increased. Since $R_s$ practically informs the amount of confidential information leaked to eavesdropper so for the higher value of variance $R_s$ approaches $R_c$. Meanwhile, increasing $\alpha$ causes $R_s$ to decrease while keeping secrecy rate $R_c$ to a particular value. This is mainly because increasing $\alpha$ causes the molecule to disintegrate rapidly, thereby causing the particle to be useless.

The analytical and simulation behaviour of generalised secrecy outage probability ($P_{out}$) for different values of degradation parameter ($\alpha$) in the uniformly distributed scenario is shown in Figure 4. From the figure, it can be observed that average fractional equivocation decreases as the variance of eavesdropper distance ($\sigma^2$) increases, out of both the parameters the effect of increasing variance is more dominant compared to $\alpha$. Moreover, the average fractional equivocation is non-zero even when secrecy rate ($R_s$) becomes zero, the expression of which can be obtained from (62) by putting $R_s = 0$. Moreover, $\Delta$ increases more prominently with increase $\alpha$. Thus, channel parameters play a major role in determining the secrecy performance of diffusive molecular communication systems.

Simultaneously, the variation of average fractional equivocation ($\Delta$) with respect to the variance of eavesdropper distance for different values of secrecy rate ($R_s$) in Gaussian distribution regime is plotted in Figure 9. From the figure, it can be visualised that $\Delta$ decreases simultaneously with respect to increasing variance as well as with increasing $R_s$. Moreover, even if $R_s$ becomes zero the average fractional equivocation ($\Delta$) is non-zero. Furthermore, simultaneous increase in the degradation parameter ($\alpha$) value causes a significant increase in $\Delta$. Thus, both channel parameters ($\alpha$ and $R_s$) play a vital role in controlling the secrecy performance of diffusive molecular communication systems.
6  CONCLUSION AND FUTURE WORK

In this work, we considered secrecy analysis of the diffusive molecular timing channel, where modulation of information is present in the time of release of particles. By assuming the upper bound on the capacity, we formally calculated the closed-form expressions for the upper bound of average eavesdropper capacity when the distance of eavesdropper was assumed to be uniform as well as Gaussian distributed. We further calculated the approximate analytical expression for the upper bound on the capacity, which shows the direct relation with the distance. We then used this approximate analysis for the calculation of various secrecy metrics. Based on the mathematical analysis, the upper bound of average eavesdropper capacity is plotted, which shows a decreasing trend with increasing variance, when the eavesdropper distance is assumed to be uniform and Gaussian distributed. Furthermore, for the comprehensive analysis of physical layer security in molecular timing channels, more robust metrics such as generalised secrecy outage probability, average fractional equivocation and average information leakage rate were used. For this, we first calculated the analytical expressions for these metric in both uniform and Gaussian distributed scenarios and then based on the mathematical results, we analytically showed the secrecy performance metrics.

Finally, from the analytical results of generalised secrecy outage probability, it can be concluded that generalised secrecy outage probability shows a decreasing trend when the eavesdropper variance is increased, wherein the decrease is more prominent with increasing degradation parameter. Similarly, the expressions for average fractional equivocation were also calculated in uniform and Gaussian distribution regimes, and the analytical results showed that the average fractional equivocation decreases with increasing variance. Moreover, we also calculated the expressions for average information leakage rate when eavesdropper distance was uniform and Gaussian distributed. Since information leakage rate characterises the amount of information leaked when the scenario of classical secrecy is not obtained, thus from the numerical analysis done, it can be easily inferred that average information leakage rate increases with increasing variance. Moreover, increasing degradation parameter causes the average information leakage rate to decreases rapidly because increasing degradation rate causes the particles to disintegrate rapidly. Similarly, the numerical results indicate that increasing the secrecy rate cause the average information rate to increase significantly.

As a part of further studies, it is desirable to focus on analysing the secrecy performance when the main channel statistics are also not known at transmitter. Moreover, the generalised secrecy analysis can further be extended on a surface, that is, when the random variable is multivariate.

REFERENCES

1. Nakano, T., et al.: Molecular communication for nanomachines using intracellular calcium signaling. In: 5th IEEE Conference on Nanotechnology, pp. 478–481. IEEE, Piscataway (2005).
2. Nakano, T.: Molecular communication: A 10 year retrospective. IEEE Trans. Mol. Biol. Multi-Scale Commun. 3(2), 71–78 (2017).
3. Nakano, T., et al.: Molecular Communication. Cambridge University Press, Cambridge (2013)
4. Sharma, G., Singh, A.: On the optimal threshold for diffusion based molecular communication system. In: 2018 2nd European Conference on Electrical Engineering and Computer Science (EECS), pp. 366–370. IEEE, Piscataway (2018).
5. Sharma, G., Singh, A.: On the distribution of molecules for diffusion based molecular communication system. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICC-CNT), pp. 1–6. IEEE, Piscataway (2019).
6. Pandey, N., et al.: Truncated levy statistics for diffusion based molecular communication. In: GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1–6. IEEE, Piscataway (2017).
7. Singh, A., et al.: Performance analysis of modulation schemes for diffusion-based molecular communication. IEEE Trans. Wirel. Commun. 14(10), 5681–5691 (2015).
8. Gine, I.P., Akylidz, I.F.: Molecular communication options for long range nanonetworks. Comp. Netw. 53(16), 2753–2766 (2009).
9. Dressler, F., Kargl, F.: Towards security in nano-communication: Challenges and opportunities. Nano Commun. Netw. 3(3), 151–160 (2012).
10. Loseni, V., et al.: Security and privacy in molecular communication and networking: Opportunities and challenges. IEEE Trans. Nanobiosci. 13(3), 198–207 (2014).
11. Mucchi, L., et al.: Secrecy capacity and secure distance for diffusion-based molecular communication systems. IEEE Access 7, 110687–110697 (2019).
12. Farsad, N., et al.: A comprehensive survey of recent advancements in molecular communication. IEEE Commun. Surv. Tutor. 18(3), 1887–1919 (2016).
13. Akylidz, I.F.: Nanonetworks: A new frontier in communications. In: Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, pp. 1–2. ACM, New York (2012).
14. Zhai, H., et al.: Bio-inspired design and implementation of mobile molecular communication systems at the macroscale. In: 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, Piscataway (2018).
15. Guo, W., et al.: Molecular versus electromagnetic wave propagation loss in macro-scale environments. IEEE Trans. Mol. Biol. Multi-Scale Commun. 1(1), 18–25 (2015).
16. Farsad, N., et al.: On the capacity of diffusion-based molecular timing channels. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 1023–1027. IEEE, Piscataway (2016).
17. Borst, A., Theunissen, F.E.: Information theory and neural coding. Nat. Neurosci. 2(11), 947–957 (1999).
18. Farsad, N., et al.: Capacity limits of diffusion-based molecular timing channels with finite particle lifetime. IEEE Trans. Mol. Biol. Multi-Scale Commun. 4(2), 88–106 (2018).
19. Pierobon, M., Akylidz, I.F.: Capacity of a diffusion-based molecular communication system with channel memory and molecular noise. IEEE Trans. Inf. Theory 59(2), 942–954 (2012).
20. Farsad, N., et al.: Tabletop molecular communication: Text messages through chemical signals. PLoS One 8(12), e82935 (2013).
21. Mucchi, L., et al.: A new metric for measuring the security of an environment: The secrecy pressure. IEEE Trans. Wirel. Commun. 16(5), 3416–3430 (2017).
22. Islam, S.R., et al.: Secure channel for molecular communications. In: 2017 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1–4. IEEE, Piscataway (2017).
23. Li, H., et al.: Capacity of the memoryless additive inverse Gaussian noise channel. IEEE J. Sel. Areas Commun. 32(12), 2315–2329 (2014).
By plotting the capacity upper bound in MATLAB it can be seen that the effect of logarithmic term and the whole expression in the negative term is more prominent compared to the term containing modified Bessel’s function. Therefore, modified expression is written as:

\[
C_{ub} \approx \ln(e) + \ln\left(\tau_{m} + \frac{\epsilon}{p}e^{-p}\right) - \frac{e^{-p}}{2} - \left(\frac{2p}{2\pi}\right)Ei(-2p) + \left(\frac{e^{-p}}{2}\right)\ln\left(\frac{e^{p}}{2\pi}\right) - \frac{e^{-p}}{2\pi}Ei(2p). \quad (A.2)
\]

Now applying the properties of logarithm and using various approximations we obtain:

\[
C_{ub} \approx 1 + d\sqrt{\frac{\alpha}{D}} + \ln(\tau_{m}). \quad (A.3)
\]

Now by substituting the expression of \(\tau_{m}\) from (8) and putting \(\tau_{x} = 1\) we have,

\[
\ln(\tau_{m}) \approx \ln(\frac{\tau_{m} + e^{-p}\sqrt{\frac{\epsilon}{2\alpha}}}{\sqrt{\frac{\epsilon}{2\alpha}}}) \approx \ln\left(e^{-d}\sqrt{\frac{\pi}{D}}\sqrt{\frac{\epsilon}{2\alpha}}\right). \quad (A.4)
\]

The approximation is valid when \(e^{-d}\sqrt{\frac{\pi}{D}}\sqrt{\frac{\epsilon}{2\alpha}}\) is small, that is, \(\ln(1 + x) \approx \ln(x)\) for \(x\) small. Thus by substituting (A.4) in (A.3) and by further solving, we obtain the approximate expression which is given as

\[
C \approx 1 + \ln(d) - \ln\left(\sqrt{4D\alpha}\right). \quad (A.5)
\]