Secrecy Performance of Diffusion-Based Molecular Timing Channels

Thesis submitted for the award of the Degree
of

Doctor of Philosophy

in the Department of Electrical Engineering

by

Gaurav Sharma
(2018REE0018)

Under the supervision of

Dr. Ajay Singh

भारतीय प्रौद्योगिकी
संस्थान जम्मू
INDIAN INSTITUTE OF
TECHNOLOGY JAMMU

Indian Institute of Technology Jammu
Jammu 181221

October 2021

Declaration

I hereby declare that the matter embodied in this thesis entitled **"Secrecy Performance of Diffusion-Based Molecular Timing Channels"** is the result of investigations carried out by me in the Department of Electrical Engineering, Indian Institute of Technology Jammu, India, under the supervision of **Dr. Ajay Singh** (IIT Jammu) and it has not been submitted elsewhere for the award of any degree or diploma, membership etc. In keeping with the general practice in reporting scientific observations, due acknowledgements have been made whenever the work described is based on the findings of other investigators. Any omission that might have occurred due to oversight or error in judgment is regretted. A complete bibliography of the books and journals referred in this thesis is given at the end of the thesis.

October 2021
Indian Institute of Technology Jammu

Gaurav Sharma
(2018REE0018)

Dedicated to my beloved parents.

Acknowledgements

First and foremost, I wish to express my deepest gratitude to Dr. Ajay Singh, my supervisor for his valuable guidance and constant support at all stages of my Ph.D study and related research. His constant encouragement to think independently has been a great source of motivation. I would have definitely not reached at this point without his support and encouragements. It was a privilege for me to work with an extraordinary supervisor like him.

I am indebted to Prof. Ranjan K. Mallik, IIT Delhi, for his inspiring guidance and encouragement for bringing this work to a logical end.

I am thankful to Dr. Nilay Pandey for time to time discussions and interactions during the course of this work.

I would also like to thank my research committee members, Dr. Ravikant Saini, and Dr. Yamuna Prasad Shukla, for their valuable comments and suggestions during my research work.

A special thanks to my family. Words can not express how grateful I am to my father, Dr. Sudershan Kumar, and my mother, Mrs. Sneh Lata Sharma for their unconditional love, support and motivation. They have always been very supportive and understanding throughout my life. I would like to thank my sister Dr. Rohini Sharma, my brother-in-law Dr. Sameer Abrol and my nephew Ridhaan for their love, support, and understanding.

I thank all the staff members of the low voltage lab for providing all the logistic support. My time spent at IIT Jammu was made memorable by the friends who were always there to help and support me. My special thanks to Shilpa Thakur, Mohit Pal, Ashwani Koul, Aditi Gupta, Sonam Gupta, Pummy Sharma, Rahul Kumawat, Swastik Gupta, Harsh Dev Singh, Surrendra Tyagi for the lengthy discussions and the enjoyable moments shared together.

Abstract

Molecular communication (MC) is an emerging bio-inspired field where the exchange of information between various nano-machines is experienced based on the chemical exchange. The chemical exchange of information molecules between transmitter and receiver enables the transmission, propagation, and reception of information systematically. Based on this, MC is proposed as a promising option for the communication of information molecules among various nano-devices in the nano-networks. Further, these nano-devices, specially called nano-machines, are used to perform various tasks such as sensing, computing and actuating at the micro- and nano-scale levels. This is motivated by the fact that MC is primarily experienced in nature, where cells implement MC for communication at intracellular and intercellular levels. Nowadays, MC finds a variety of applications in biological environments, especially in human healthcare scenarios, where MC can be used for target drug delivery, human body monitoring, defense, industrial applications and lab on chip. In MC based nanonetworks, most of the work have been devoted to the information-theoretical foundations. Secure transmission of information from the transmitter to the receiver is an essential task in any communication system. Being a new area of research most of the work in MC is being carried out to find communication models using biologically compatible components. Therefore, an important aspect concerning security has not been rigorously investigated. Secrecy is a major concern in MC as the nano-devices would be implemented in a biologically compatible environment where there is a plethora of privacy-sensitive information. Therefore, it becomes extremely important that the security issues in the MC paradigm are addressed at the very start rather than adding secrecy to the MC systems at the later stage.

The focus of this Ph.D. thesis is to address the secrecy concern in the diffusion based molecular timing (DBMT) channels. In the thesis, we have employed free diffusion for the propagation of information particles. The objectives of the research presented in the thesis are to analyze the secrecy performance of DBMT channels by employing various secrecy performance metrics. For this, we first calculated the upper bound on the average eavesdropper capacity of a single particle DBMT channels when the distance of the eavesdropper is uniform and Gaussian distributed. Second, we analyzed the secrecy performance of single-particle DBMT channels in the partial secrecy regime using various secrecy performance metrics such as generalized secrecy outage probability (GSOP), average fractional equivocation and average information

leakage rate. Third, we optimized various secrecy performance metrics and calculated various optimal transmission rates, which would minimize GSOP, maximize average fractional equivocation, and minimize average information leakage rate. Fourth, we examined the secrecy from confusion level perspective by calculating the amount of confusion level expression. Fifth, we explored the system's secrecy from the secrecy loss perspective, where we calculated the amount of secrecy loss in multi-particle DBMT channels. The analytical results presented in the thesis were also validated by undertaking particle-based simulations. The research undertaken in the thesis provides a fundamental framework to implement secrecy in DBMT channels by analyzing the effect of an eavesdropper in the DBMT channels. This work would further help to bridge the gap between theoretical and practical aspects in MC based systems.

Contents

List of Figures

List of Tables

List of Symbols

Symbol	Description
D	Diffusion coefficient
μ^2	Micrometer sq.
s	Seconds
k_B	Boltzman constant
T	Temperature in Kelvin
η	Dynamic viscosity
R_H	Stokes radius
X_m	Size of propagating molecules
S_{media}	Size of media molecule
P	Code length
O_i	ith-channel output
$\mathscr{I}$	Message set
ε	Encoder function
φ	Null Set
ν	Decoder function
d	Distance travelled
d_E	Distance travelled towards Eve
d_M	Distance travelled towards Bob
t	Time coordinate
r	Radius of absorbing receiver
C	Concentration of molecules
x, y, z	Cartesian coordinate system
M_0	Number of molecules released by point source

Symbol	Description
v	Flow velocity
$f_X(x)$	Probability density function
$F_X(x)$	Cumulative distribution function
τ_x	Symbol interval
τ_s	Slot duration
c	Lévy noise parameter
τ, τ_n	Particle lifetime
μ	Mean or location parameter
μ_x	Mean of eavesdropper distance
μ_M	Mean of molecules received at eavesdropper
σ_x^2	Variance of eavesdropper distance
σ_M^2	Variance of molecules received at eavesdropper
T_t, T_x	Transmission time
T_a, T_y	Arrival time
T_n	Propagation delay
α	Degradation rate
$h(\tau)$	Exponential modelled decaying rate
t_d	Lévy distributed random variable
C_{ub}	Capacity upper bound
C_{lb}	Capacity lower bound
C_b, C_B, C_M	Main or Bob channel capacity
R_b, R_B	Main or Bob Rate
C_e, C_E	Eavesdropper capacity
C_s, C_S	Secrecy capacity
R_s, R_S	Secrecy rate
X	Main signal
Y	Received or observed signal
Z	Signal received at eavesdropper
$\ln(.)$	Natural logarithmic function

Symbol	Description
p	Scaled version of Lévy noise parameter
$I_{1/2}(.)$	Modified Bessel's function of first kind
$K_{-3/2}(.)$	Modified Bessel's function of second kind
$Sinh(.)$	Hyperbolic sinusoidal function
π	Pi
μ_x	Mean of Eve's distance
σ_E^2	Variance of Eve's distance
Ei	Exponential integral
$\frac{\delta}{\delta t}$	Partial differentiation
$\bigtriangledown^2$	Laplacian operator
d_E	Eavesdropper distance
d_M	Bob distance
$\mathscr{U}$	Uniform distribution
$\mathscr{N}$	Gaussian distribution
$\gamma(.)$	Lower incomplete Gamma function
δ	Eve's decoding error probability
P_{out}	Secrecy outage probability
Δ	Fractional equivocation
$\bar{\Delta}$	Average fractional equivocation
R_L	Average information leakage rate
$\mathbf{E}$	Expectation operator
G_c	Coding gain
G_d	Diversity order
L	Bernoulli distributed RV
k'	Normalizing factor
p_τ	Hitting probability
N	Number of molecules
M_E	Number of molecules received at Eve
M_B	Number of molecules received at Bob

Symbol	Description
k	Bob (B), Eve (E)
$Q(.)$	Gaussian Q-function
Ca^{+2}	Calcium ions
K^{+1}	Potassium ions
n	n-vector

List of Abbreviations

Abbreviation	Description
1-D	1-Dimensional
2-D	2-Dimensional
3-D	3-Dimensional
ACL	Amount of confusion level
AIGN	Additive inverse Gaussian noise
AoF	Amount of fading
ASL	Amount of secrecy loss
ASR	Average secrecy rate
ATP	Adenosine triphosphate
BANA	Body area network authentication scheme
BCSK	Binary concentration shift keying
BER	Bit error rate
Bio	Bilogical
C	Capacity
CDF	Cumulative distribution function
CFARD	Clock free asynchronous receiver design
CSI	Channel state information
CSK	Concentration shift keying
DBMT	Diffusion-based molecular timing channels
DNA	Deoxyribonucleic acid
EM	Electro-magnetic
Eve	Eavesdropper

Abbreviation	Description
erf	Error function
FA	First arrival
FET	Feild effect transistor
G-SNR	Geometric-signal to noise ratio
GSOP	Generalized secrecy outage probability
GSS	Golden section search
ICW	Intercellular calcium wave
iid	Independent and identically distributed
IG	Inverse Gaussian
IoBNT	Internet of bio-nano things
IRSK	Isomer-based ratio shift keying
ISI	Inter symbol interference
IP_3	1,4,5-triphosphate
KDR	Key disagreement rate
LAF	Linear average filter
LTI	Linear time invariant
MAP	Maximum a posteriori
MARCO	Molecular array based communication
MC	Molecular communication
MCSK	Molecular concentration shift keying
MEMS	Micro-electro-mechanical systems
ML	Maximum-likelihood
Ml	Machine learning
MoSK	Molecular shift keying
MT	Molecular timing
MTSK	Molecular transition shift keying
NEMS	Nano-electro-mechanical systems
nm	Nanometer
OOK	On-Off keying

Abbreviation	Description
PAM	Pulse amplitude modulation
PPM	Pulse position modulation
PLS	Physical layer security
p.d.f	Probability density function
$\mathbb{P}$	Probability
RDMEX	Reaction-diffusion master equation with exogenous input
RNA	Ribonucleic acid
RSS	Received signal strength
RV	Random variable
SNR	Signal to noise ratio
SOP	Secrecy outage probability
TEC	Time-elapse communication
THz	Terahertz
UN	Unintended nanomachine
URN	Unintended receiver nanomachine
UTN	Unintended transmitter nanomachine

Chapter 1

Introduction

1.1 Background

The process of transfer of information from the transmitter to the receiver has always been a significant part of the human race. In the present era, modern-day communication schemes solve the problem of information exchange by deploying the electrical to electromagnetic (EM) signals in the radio to optical spectrum. However, there are still many areas where conventional radio-based communication does not provide promising results. Some of the application areas where radio-based communication fails are saltwater environments, pipeline networks, underground mines, or tunnels [1]. Particularly EM wave suffers from diffraction when they travel through the saline water environment [2]. Moreover, with the advancements in the field of nanotechnology, it is now possible to develop and deploy nanoscale 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 because of the constraints in the antenna size [3, 4]. For such microscale environments, molecular communication (MC), where information is exchanged chemically by exchanging information molecules, has emerged as a promising communication option [5], [6], [7]. The following are some of the basic differences between the conventional EM wave-based communication and the MC scenario [8]:

- MC systems are mostly applied in microscale as well as macroscale environments. In contrast to the classical communication systems, the complexity of the encoder and decoder circuits is a major problem in many microscale MC environments. Since nanode-

vices are resource-limited devices usually employed for communication at the nanoscale. Therefore, it becomes imperative to analyze the theoretical framework of the MC environments where these nanodevices are utilized for communication. Compared to conventional radio-based communication, in MC, simpler and mathematically tractable models are usually used for encoders and decoders. In conventional radio-based communication, the fundamental goal of coding theory is to determine the practical capacity of the system while using less complicated encoder and decoder circuits. So in order to analyze the computational features of MC environments, various molecular circuit models are defined.

- Most of the MC environments are influenced by the physical aspects of the transmitting and receiving devices. The change in the physical behaviour of the transmitter and the receiver may change the channel statistics even in the absence of channel noise. For example, an imperfection in the transmitter's response to a stimulus leads to a random generation of information particles with a certain mean and variance. Similarly, the sensing noise at the receiver has a variance which is a function of signal amplitude. Therefore, increasing the signal's amplitude, the variance of the sensing noise increases. Further, due to the mobility of the transmitter and receiver, certain chemicals are released in the MC environment, which modifies the system's statistics.

- Analogous to frequency usage in the conventional EM wave-based communication systems in MC, usually different types of molecules are employed. However, unlike the EM spectrum in MC, the presence of different types of molecules leads to the chemical interactions among them, which in turn causes non-linearity in the channel. Moreover, due to the presence of different types of molecules in the channel, the reception process becomes challenging.

- Due to the LTI (Linear Time-Invariant) nature of the conventional EM wave-based system the mathematical tools such as linear algebra and Fourier transforms can be readily applied to these systems. Although the diffusion process at the macroscale level, under stable conditions, follows LTI nature, the mathematical tools readily used in EM wave-based communication cannot be applied directly to the MC environment. This is majorly due to the non-negative nature of molecular concentration in the time domain. Due to the non-negative number of molecules in the environment, the equivalent Fourier analy-

sis (both series and transform) function in the frequency domain is not available, which further complicates the analysis of the system. Further, at the microscale level, the non-linearity of the differential equation of the diffusive chemical reactions prevents the use of various linear mathematical tools.

- Compared to the conventional EM wave-based communication systems in the MC scenario, energy is needed for the generation of the information molecules. Although the capacity of the MC channel can be increased by increasing the concentration, but this enhances the energy consumption of the system. Therefore, for an environment where there are energy restrictions, other MC channels need to be employed. The same analogy can be obtained for the EM wave-based systems, as it is well known that considerable energy is needed to reach Shannon's capacity.

- In the case of diffusive MC channels, the propagation rate of molecules is comparatively slow, which makes mathematical modelling challenging. Due to the slow propagation of the molecules in the diffusive environment, the channel state information (CSI) of the channel cannot be obtained. Moreover, the channel also suffers from inter-symbol interference (ISI), and due to non-negative molecular concentration, the conversion of the ISI channel to a memoryless channel using Fourier transform is not possible.

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 [9, 10]. In the natural systems, chemical signals are usually employed for the information transfer in intercellular and intracellular environments at the microscale and nanoscale [11], whereas the pheromones are usually employed by social insects for the long-range communication [12]. Therefore, inspired from nature, in MC, transmitting nanomachines releases information molecules or lipid vesicles in the aqueous or gaseous media. These molecules then travel through the channel and are received at the receiving nanomachines. Unlike radio-based communication, the noise in MC also degrades information at the receiving nanomachine. In MC, the sources of noise are [6]:

- Random Propagation Noise or diffusive noise

- Emission noise by the transmitter

- Reception noise or the counting noise

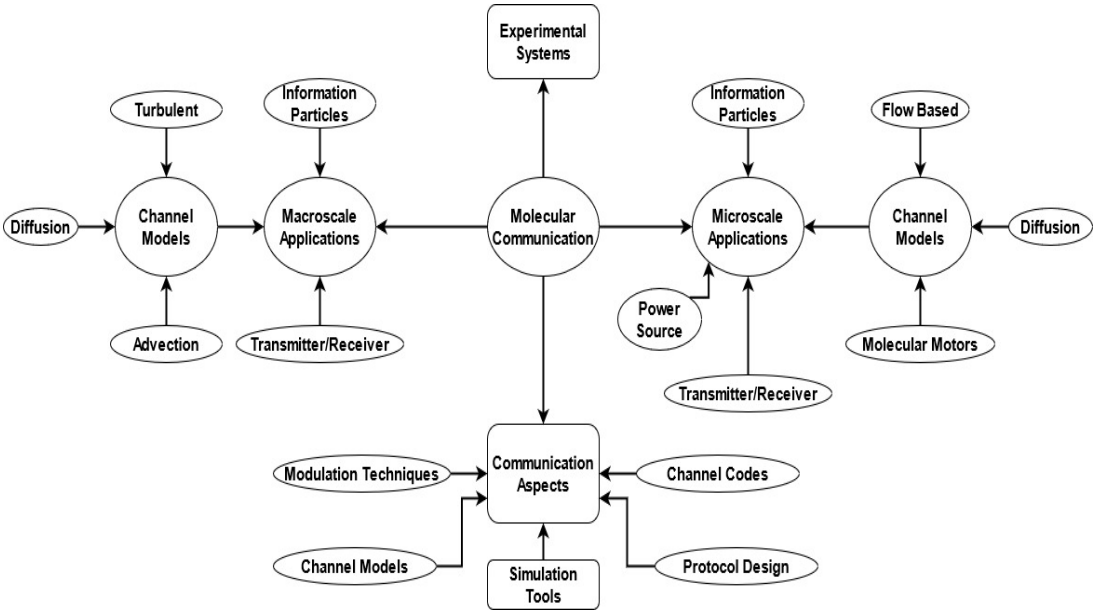

Figure 1.1: General scenario of molecular communication.

- Environmental noise due to degradation process
- Multiple transmitters.

In most of the conventional wireless communication scenarios, the signal is transmitted by the transmitter, which after propagating through the channel media, is received by the receiver. At the receiver, the received signal is demodulated first and then subsequently decoded via channel decoders. The role of the channel decoders is to estimate the message symbols which, after propagating through the media, have become erroneous. After successful estimation, the receiver retrieves the information transmitted by the transmitter, thereby achieving successful communication. In contrast to conventional EM wave-based communication in MC, the generation of information molecules from the transmitter is accomplished by a physical process. Further, a processing unit is required at the transmitter, which controls the mechanism for the release of particles. The processing unit present at the transmitter can perform its operation either chemically or electrically. Therefore, the transmitted information molecules are released into the channel from where they are propagated via various natural or artificial propagation processes towards the receiver. A generalized scenario of the current MC system from the application point of view is indicated in Figure 1.1. In the subsequent subsections, we will highlight various physical and chemical processes present in the MC environment that facilitate communication.

1.1.1 Information Molecules at Microscale and Macroscale

Compared to EM wave-based communication, where EM waves are employed to communicate between transmitter and receiver, information molecules or particles are the primary components in MC. The structural dimension of the information molecules governs how they propagate in the channel. Increasing or decreasing the dimensional size of the molecules affects the diffusion coefficient and hence the diffusion process in the MC scenario. So for a reliable MC channel, the information molecules should be chemically stable, robust against environmental noise and should not be affected by interference from other adjacent molecules. Moreover, due to some inherent natural processes, the information molecules also experience molecular degradation in the environment. This molecular degradation process is mainly responsible for molecular diversity at the transmitter. In many microscale biological systems, information molecules such as hormones, pheromones, deoxyribonucleic acid (DNA) and ribonucleic acid (RNA) molecules are used to carry information. However, detecting a single molecule at the macroscale is difficult, so a concentration of gaseous or chemical or liquid molecules is used for information transfer.

1.1.2 Propagation of Molecules at Microscale and Macroscale

The transmission of information from the transmitting nanomachine to a receiving nanomachine is achieved by modulating certain characteristics of the information particles. These characteristic features are mainly time of release [7], concentration [6], number [13], position [14], or type [15]. Moreover, the information can be propagated from the transmitter to the receiver via pure diffusion [16], flow assisted diffusion [17], molecular motors [18], and engineered bacteria [6]. The channel is usually an aqueous medium connecting the transmitter to the receiver in a diffusion-based MC channel.

1.1.2.1 Propagation by Simple Diffusion

The random motion which leads to the collision of one set of particles to another set of particles present in the vicinity of one another is referred to as the Simple Diffusion process. 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 [19]. Because of the random propagation, the molecules travel by utilizing the

thermal energy of the channel environment. Therefore, the diffusion-based approach does not require an additional external source of energy. In many fundamental biological processes, usually simple diffusion is observed when the particle needs to propagate from the transmitting side to the desired destination. For example, in the case of neuromuscular junctions, to convey motor action messages inside the muscle cells, the neurons emit Acetylcholine (ACh) molecules. So whenever a specific muscle needs to be contracted at a particular location in the body, then these ACh molecules are released by neurons towards muscle tissue via neuromuscular junctions [20]. Simultaneously, the same phenomenon in the case of the DNA segment is observed where the DNA molecules known as repressors propagate through simple diffusion over the DNA segment in search of a binding site [21]. The process of free diffusion can be simulated by employing Monte Carlo simulations. Particularly, the molecular motion can be modelled using discrete-time duration interval given as Δt. Mathematically, Brownian motion can be modelled as

$$(x_j, y_j, z_j) = (x_{j-1}, y_{j-1}, z_{j-1}) + (\Delta x_i, \Delta y_i, \Delta z_i) \tag{1.1}$$

where x_j, y_j, z_j represents position cartesian coordinates of the particle, Δx_i, Δy_i and Δz_i are random displacements that are Gaussian distributed ($\mathcal{N}(\mu,\sigma^2)$) with mean μ and variance σ^2. In diffusion-based MC channels, the diffusion coefficient (D) plays a major role in the information particle propagation. For a given environment, D is mathematically expressed as

$$D = \begin{cases} \frac{k_B T}{6\pi\eta R_H}, & if \quad X_m \gg S_{media} \\ \frac{k_B T}{4\pi\eta R_H}, & if \quad X_m \approx S_{media}, \end{cases} \tag{1.2}$$

where $k_B = 1.38\text{x}10^{-23}$ J/K is the Boltzman constant, T is the temperature (in Kelvin), η is the dynamic viscosity, R_H is the Stokes radius, X_m is the size of the propagating molecules and S_{media} is the size of media molecule. In many practical scenarios, the D is assumed to be stationary throughout the media with elastic collisions in the environment. The Table 1.1 represents the practical value of D.

Table 1.1: Diffusion coefficient of molecules in water [6].

Molecules	**Diffusion coefficient (D in μ^2/s)**
DNA	0.81 to 53
Human serum albumin	61
Insuline	150
Sucrose	520
Glucose	600
Glycerol	930
Nitrate	1700

1.1.2.2 Diffusion Based on Hitting Process

In most of the natural application the receiver removes the information molecules from the environment by acting as a sink or through some chemical reactions [22]. Mathematically, this process of removal of information molecules from diffusive environment can be modeled as the first hitting probability. For the 1-dimensional (1-D) environment the expression for the hitting process is given as

$$f_{hit}^{\text{1-D}}(t) = \frac{d}{\sqrt{4\pi D t^3}} \mathrm{e}^{-d^2/4Dt}, \tag{1.3}$$

where d and D represents the distance travelled and diffusion coefficient, respectively [23]. Similarly, for 3-Dimensional (3-D) environment the expression for the hitting process is formulated as

$$f_{hit}^{\text{3-D}}(t) = \frac{r}{r+d} \frac{d}{\sqrt{4\pi D t^3}} \mathrm{e}^{-d^2/4Dt}, \tag{1.4}$$

where r is the radius of the absorbing receiver, d represents the distance and D represents the diffusion coefficient [24]. Now based on the expression of the 3-D hitting process obtained in (1.3), the expression of fraction of molecules hitting until a certain time (t) can be obtained by integrating the f_{hit}^{3-D} expression as given in (1.4). It should also be noted that as $t \to \infty$ the probability of molecules not hitting the absorbing receiver becomes positive. For a 2-D environment the hitting probability is not available in the MC literature. Therefore asymptotic analysis is usually employed to calculate the hitting rate [25]. However, in case of planar wedge environment the hitting process expressions can be obtained in terms of wedge angles [26].

1.1.2.3 Diffusion at Macro-scale Level

At the macro scale level, rather than sending a single or few molecules, a large number of molecules are used for the information transfer. So in order to model this, it is better to write a diffusion equation that allows the user to model the statistical movement of the randomly moving molecules. The partial differential equation, which represents the diffusion process, is expressed as

$$\frac{\partial C}{\partial t} = D\nabla^2 C, \tag{1.5}$$

where ∇^2 express the Laplacian operator, D is the diffusion coefficient, and C is the concentration at a particular spatial-temporal location. Consequently, C can be represented as the function of x, y, z and t respectively. To solve (1.5), different initial conditions can be employed. Therefore, the mathematical expression of C, which is a function of x, y, z and t, is represented as

$$C(x,t) = \frac{M_0}{\sqrt{4\pi Dt}} \exp\left\{-\frac{x^2}{4Dt}\right\}, \tag{1.6}$$

$$C(x,y,t) = \frac{M_0}{\sqrt{4\pi Dt}} \exp\left\{-\frac{x^2+y^2}{4Dt}\right\}, \tag{1.7}$$

$$C(x,y,t) = \frac{M_0}{\sqrt{4\pi Dt}} \exp\left\{-\frac{x^2+y^2+z^2}{4Dt}\right\}, \tag{1.8}$$

where M_0 is the number of molecules released by point source at $t = 0$. Based on the diffusion equation the channel impulse response can be derived for the environment with an absorbing receiver [25]. Simultaneously the diffusion equation can also be solved by utilizing different initial conditions [21].

1.1.2.4 Propagation Based On Flow

Although diffusion is a promising option for the information transfer in energy constraint environment, however the diffusion process can be slow process. Therefore, to overcome this challenge one way is to introduce flow into the environment. The molecules travel with certain flow velocities, which are a function of space and time, and are received at the receiver. For example in case of human biology certain glands secrete hormones that are propagated towards the desired destination with the help of flow in the blood stream. Similar to diffusion process the flow based propagation of information molecules can be artificially simulated using Monte

Carlo simulations. Mathematically the expressions for flow based environment are

$$\begin{aligned}\Delta x_j &= v_{x,j-1}(x_{j-1},y_{j-1},z_{j-1})\Delta t + \mathscr{N}(0,2D\Delta t),\\ \Delta y_j &= v_{y,j-1}(x_{j-1},y_{j-1},z_{j-1})\Delta t + \mathscr{N}(0,2D\Delta t),\\ \Delta z_j &= v_{z,j-1}(x_{j-1},y_{j-1},z_{j-1})\Delta t + \mathscr{N}(0,2D\Delta t),\end{aligned} \tag{1.9}$$

where $v_{x,j-1}(x_{j-1},y_{j-1},z_{j-1})$, $v_{x,j-1}(x_{j-1},y_{j-1},z_{j-1})$ and $v_{x,j-1}(x_{j-1},y_{j-1},z_{j-1})$ are flow velocities and are a function of space and time.

1.1.2.5 Flow At Macroscale

Practically, the process of diffusion is very slow, even at the macroscale level. Therefore, in order to speed up the process of information transfer, a flow-based phenomenon is introduced along with the diffusion process. When flow is present in the channel environment, the diffusion equation in (1.5) gets modified, and this modified equation is known as the advection-diffusion equation (also known as the diffusion with drift) [27], [28]. Mathematically, the modified version of (1.5) is obtained as

$$\frac{\partial C}{\partial t} + \nabla.(vC) = D\nabla^2 C, \tag{1.10}$$

where v is the flow velocity. Note that the D in the above equation can be assumed to be fixed and in case where D varies spatially the analytical solution can also be obtained for the (1.10) as given in [29]. The solution of the above partial differential equation in (1.10) by utilizing initial conditions is

$$C(x,t) = \frac{M_0}{\sqrt{4\pi Dt}}\exp\left\{-\frac{(x-vt)^2}{4Dt}\right\}, \tag{1.11}$$

where v is the speed in the positive x direction. The expression (1.11) is obtained for the 1-D system. Though most of the mathematical reasoning and theoretical framework of conventional communication can be used to characterize MC systems, certain aspects of MC are fundamentally distinct from EM wave-based communication. The advection-diffusion equation obtained in (1.10) can be employed at the microscale level also. However, the characteristic features, especially the flow of the media, of the microscale and the macroscale environments are entirely different. In the case of microscale environments, the flow is usually laminar, but for the macroscale environment, the flow is turbulent.

1.1.2.6 Propagation via Molecular Motor

In addition to diffusion and flow-based propagation mechanisms, molecular motors are another method by which the information molecules can be transported from the transmitting source to a receiver destination. One of the typical examples of molecular motor-based propagation is the Kinesin protein molecule which walks over microtubule tracks [30]. Microtubules are tubular structures that are hollow from inside with walls made up of protofilaments. The microtubules are the polymerized structures primarily composed of $\alpha-$ and $\beta-$tubulin joined as dimeric subunits. Naturally, in the biological environment, the microtubules are found in the cytoskeleton structures of the cytoplasm, which then helps achieve various intracellular and intercellular operations. Similarly, the kinesin protein molecule consists of a head, neck, stalk and tail. The head part of the Kinesin is attached to the microtubule, the neck portion is used to provide the necessary support to the protein molecule, the stalk joins the neck and a tail portion, and finally, the tail acts as a connection portion that attaches protein molecule to the desired entity. For example, consider the case of hydrolysis of adenosine triphosphate (ATP), where the release of phosphate from ATP produces energy resulting in the motion of the head domain of the kinesin protein molecule in one direction along the microtubule track. This motion of kinesin protein molecule over microtubule structure can be modelled as a 1-D motion by neglecting probability of detachment [31]. Mathematically, the displacement of molecular motor over a time interval Δt is given as

$$l_j = l_{j-1} + v_a \Delta t, \tag{1.12}$$

where l_j is the location of kinesin protein molecule at jth simulation step and v_a is average velocity.

1.1.2.7 Propagation by Mobile Microtubule

Compared to the previous propagation scenario where the kinesin molecule move over a stationary microtubule structure, in this propagation scenario, the stationary kinesin molecules connected to a substrate leads to the motion of microtubular filaments. This type of propagation mechanism is beneficial in the case of lab-on-a-chip where the transmitting and receiving nanomachines are present on the same chip [32]. However, compared to kinesin molecules that inherently can carry information material, the microtubule filaments require a certain mechanism for carrying information particles. In biology, the information-carrying mechanism is

achieved through DNA hybridization wherein the information particles (vesicles) are carried via hybridization of DNA bonds [30]. Particularly, a single DNA strand is composed of nucleotides which in turn are created using four nucleobase compounds: adenine, guanine, thymine, cytosine. These nucleobases combine through various hydrogen bonds, which then leads to the formation of two single-stranded DNA. These single-stranded DNA structures are used as a cover material over vesicle particles, transmitting devices, and receiving devices. Further, the microtubules are covered with 15 DNA strands which, on coming in contact with the vesicle particles covered with 23 DNA strands, hybridize and then transfer information to the destination. The whole process can be modelled via Monte Carlo simulations. The microtubules movements are mostly systematic and particularly in x-y directions only. Mathematically the motion of microtubules is expressed as

$$\begin{aligned} x_j &= x_{j-1} + \Delta r_j \, Cos\theta_j, \\ y_j &= y_{j-1} + \Delta r_j \, Cos\theta_j, \end{aligned} \tag{1.13}$$

where x_j, y_j, Δr_j and θ_j are the x-y coordinates, step size and directional angle in which motion occurs respectively.

1.1.2.8 Propagation Through Bacteria

Recently, in many practical applications, bacteria-assisted propagation is being used to propagate information molecules from a source to a destination. In a bacteria-based approach, the messenger molecules are embedded inside a bacteria at the source. The bacteria's embedded with information are then released into the environment, where they are propagated throughout the channel until they reach their destination and transfer the message. In bacteria-assisted propagation, flagellated bacteria is used, which is self-propelled, comprising a filament known as flagellum and a motor that acts as a propeller. The receiver releases some sort of attractant molecules in the environment, leading to a concentration gradient. Based on the concentration gradient, these flagellated bacteria are attracted towards the receiver. Mathematically, the displacement of bacteria due to concentration gradient is expressed as

$$\Delta r_j = v_j^r \, T_j^r, \tag{1.14}$$

where Δr_j, v_j^r and T_j^r denote displacement, velocity and run duration for the jth run. When there are no attractant molecules then T_j^r (run duration) and T_j^t (tumbling duration) are distributed exponentially with λ_r and λ_t being the mean values of exponential distributions. However, in the attractant molecules environment, the value of λ_r increases depending on the concentration of the molecules. Moreover, when the flagellated bacteria is in the state of motion, they usually travel in a particular direction. Nevertheless, due to rotational diffusion, a small deviation is observed in the locomotive process, and this deviation can be modelled using a Gaussian process with 0 mean and $2D_r t$ as the variance [21], [33].

1.1.2.9 Gap Junction Propagation

Another example of a practical propagation mechanism found at the microscale level is the gap junctions propagation approach. Gap junctions are the intercellular connections present between neighbouring cells situated at the membrane of the cell. Gap junction facilitates the motion of selected particles between two neighbouring cells via free diffusion. The permeability of the gap junctions varies with time, enabling various molecules to pass through them. In biology, the use of the intercellular calcium wave (ICW) mechanism for the propagation of information is an example of gap junction propagation. In the ICW propagation mechanism, the concentration of Ca^{+2} ions increases after a stimulus is applied to the cell. Increased Ca^{+2} concentration then passes through the adjacent cells leading to diffusion of ATP molecules or the 1,4,5-triphosphate (IP_3) molecule [34].

1.1.2.10 Propagation via Neurochemical Process

In many neurochemical processes, neurotransmitters are used to transmit signals from a neuron to the desired cell. Neurotransmitters are basically endogenous chemicals that are loaded into the pre-synaptic side of the synapse. Subsequently, these neurotransmitters are then released into the environment, where they diffuse and bind to the destination's sheath. One such biological environment where the neurotransmitters are used is in the neuromuscular junctions. Neuromuscular junctions is a semi-closed structure present in between a neuron and muscle cell. Whenever a muscle in a particular part of the body needs to be contracted, the neurons present in that area transmits a signal through neurotransmitter. Table 1.2 shows the tabular representation of various propagation schemes in MC.

Table 1.2: Various propagation schemes in MC [6].

Propagation Scheme	**Based On**	**Information Carrier**	**Energy Requirement (in propagation)**
Diffusion without flow	Diffusion	Molecules	0
Diffusion with flow	Diffusion + Flow	Molecules	Flow require energy
Molecular Motor over Microtubules	Molecular Motor	Vesicles	1 Adenosine triphosphate for 8nm
Microtubules over Molecular Motor	Molecular Motor	Vesicles	1 Adenosine triphosphate for 8 nm
Bacteria Assisted	Bacteria	Bacteria	Bacteria movement requires energy
Gap Junction	Diffusion + Gates	Molecules	Gate triggering requires energy
Neurochemical	Diffusion + Enzymes	Molecules	0

1.1.3 Transmitter Receiver Mechanisms for Microscale and Macroscale MC

In a microscale MC environment, the dimension of the transmitting device and the receiving device can be up to a few nanometers. Both the transmitting nanomachine and the receiving nanomachine can be artificially produced or by altering a cell genetically. The transmitting nanomachine primarily comprises a generation unit, a controlling unit, and a unit for processing. Likewise, the receiving nanomachine requires a detection unit for molecules sensing and a processing unit for decoding and deciphering the information. The processing unit present in the transmitter and the receiver can be realized with the help of logic gates and memory elements. In the processing unit, information molecules can be created by modifying a particular pathway, leading to the release of signalling molecules. A synthetic oscillator can release information molecules generated inside the processing unit at a particular instant of time. Naturally, the information is received through protein structures known as chemical receptors. These chemical

receptors are basically protein structures that attach themselves to a specific ligand through ionic or hydrogen bonding. These ligand structures remove the information molecules from the environment after the detection process is accomplished [22]. Similar to the microscale MC environment, in a macroscale MC environment, the transmitting device comprises a storage container, a generation mechanism for particle generation and a controller to regulate the supply of information particles. Simultaneously, on the receiver side, a chemical sensor could be used for the detection of information molecules. Further, in contrast to the microscale environment at macroscale scenario, the processing unit can be a high-end computing device or a microcontroller, depending on the area where they have to be installed [35].

1.1.4 Power Source

Analogous to the EM wave-based communication systems in the MC environment for proper operation of the transmitter, receiver and propagation mechanism external source of power is required. At the microscale level, the power is harvested from the environment itself. For example, the diffusion process derives power from the thermal energy prevalent in the environment. Meanwhile, the transmitter and receiver may employ chemical reactions for information transfer or rely on specific molecules present in the environment. Since an external power source may not be employed at the microscale level because of the dimensionality constraints, however, at the macroscale level, the use of an external power source may boost the performance of the MC systems. At the macroscale level, the power sources can be electrical, mechanical or solar.

1.1.5 Various Modulation and ISI Mitigation Techniques

In MC, the information is modulated based on concentration or the number of molecules, type or structure of molecules and the time of the release of molecules. Particularly in the timing-based approach, the information to be transmitted is encoded at the time of release of information molecules [36]. In a concentration based modulation scheme, a bit-0 is represented when no concentration of molecules is transmitted, and a bit-1 is represented when the transmitter releases Q concentration of molecules in the MC environment. This type of modulation scheme is analogous to the *on-off keying* (OOK) of the conventional radio-based communication system [37]. The modulation scheme in which the concentration of molecule is varied in accordance to the variation in the frequency or amplitude of the sinusoidal carrier signal is known as the *con-*

centration shift keying (CSK) [13]. In concentration shift keying, the transmitted symbols are encoded in the number of molecules transmitted by the transmitter. Another type of modulation scheme is in which the transmitted symbols are encoded in the type of the information molecule transmitted by the transmitting device. This type of modulation scheme is known as the *molecular type shift keying* (MoSK) [13]. Hydrofluorocarbon based information particles are the primary examples of MoSK based modulation schemes. Meanwhile, for MC inside the body, an isomer based modulation technique known as the *isomer-based ratio shift keying* (IRSK) is implemented [38]. In IRSK, information is usually encoded in the ratio of the two isomers. Similarly, in the case of continuous diffusion models, the information is modulated based on the response pulses of the system, and these types of modulation schemes are widely known as *pulse amplitude modulation* (PAM) and *pulse position modulation* (PPM). In the PAM scheme, bit-1 denotes the presence of pulse at the start of a bit interval, whereas a bit-0 represents the absence of a pulse. On the contrary, the PPM scheme is based on the phenomenon where a bit interval is divided into two equal halves where the first half represents bit-1 and the second half represents the subsequent second half [39]. In addition to the above modulation schemes, the information can also be encoded at the time of the release of the information molecules. Moreover, the modulation of information molecules on the *time of release* is analogous to the pulse position modulation technique. In order to attain higher data rates, the hybrid combination of type-based and timing-based modulation is usually implemented [40]. In the case of on-chip bacterial communication networks, usually time-elapse communication (TEC) is employed for the modulation of information. In the TEC approach, information is encoded in between the time interval of the two consecutive pulses [41]. The TEC technique usually exceeds in terms of performance when compared to the OOK method. Due to residual molecules in the MC environment, the MC channels usually suffer from ISI, which leads to memory in the channel. Therefore, it becomes important to consider ISI in the system, so all the aforementioned modulation schemes should contemplate various methods to mitigate ISI in the MC. For this, a new type of modulation scheme known as the *molecular transition shift keying* (MTSK), which is a combination of CSK and MoSK, is usually employed to reduce ISI [42]. Further, to reduce ISI in the MC environment, enzymes present in the environment can be employed. The enzymes usually degrade information particles' motion in the MC environment and hence reduce ISI in the system. Another modulation technique that reduces the ISI problem in the MC environment is based on the order of information particles. This type of modulation technique where infor-

mation is encoded in the order of the information particle is known as *molecular array-based communication* (MARCO). In MARCO, bit-0 is represented by emitting particles in the order of x succeeded by y, while bit-1 is represented by emitting particles in the order of y succeeded by x [43]. Simultaneously, another method to reduce ISI comprises of sequencing of different types of molecules in which certain types of molecules are transmitted in odd time slots while another type of molecules is released during even time slots [44]. Table 1.3 represents various modulation schemes based on which information can be transmitted in the MC environment.

Table 1.3: Different modulation schemes [6].

Name	**Abbereviation**	**Based On**	**ISI Reduction**	**Molecule Types**
On-Off Keying [37]	OOK	Concentration	No	1
Concentration Shift Keying [13], [45]	n-CSK	Concentration	No	1
Molecular Shift Keying [13], [45]	n-MoSK	Molecule Type	Moderate	n
Isomer-based Ratio Shift Keying [38]	n-IRSK	Molecule Type and Ratio	Moderate	n
Pulse Amplitude Modulation [39]	PAM	Concentration	No	1
Pulse Position Modulation [39]	PPM	Time of Release	No	1
Emission Time-based Modulation [23], [40]	-	Time of Release	No	1
Time-Elapse Communication [41]	TEC	Time of Release	No	1
Molecular Transition Shift Keying [42]	n-MTSK	Molecule Type and Concentration	Yes	2n
Molecular Array Based Communication [43]	n-MARCO	Molecule Order	Yes	n

Name	Abbereviation	Based On	ISI Reduction	Molecule Types
Molecular Concentration Shift Keying [44]	n-MCSK	Molecule Type and Concentration	Yes	2n

Another critical aspect of MC systems is the demodulation and the detection process done at the receiver. Different modulation techniques require a different set of demodulation processes. For example, in the case of frequency shift keying, the receiver employs a circuit composed of interconnections of enzymes [46]. On similar grounds, optimal receivers have been used, which minimizes the error probability of the detection process by using MAP criteria [47]. Likewise, the MAP criteria is also employed for the BCSK modulation schemes [48]. Furthermore, the ML and MAP criteria are employed for the receiver design in those systems where modulation technique used OOK and a propagation mechanism is diffusion only.

1.1.6 Applications of MC at Microscale and Macroscale

Nowadays, MC is looked up as a potential candidate in medical applications, especially in the areas of lab-on-chip devices, cell-on-chip devices and target drug delivery. In addition to these applications MC at microscale is also applied in the area of computational biology [49], environmental control and preservation [50], control and detection of chemical reactions [51] and nanobot communications [52]. In the field of medical sciences, MC is conceived as a primary candidate for the development of an artificial immune system in the body. In artificial immune system applications, small man-made devices would be injected inside the body to perform collective and individual operations. For example, one nanomachine is assigned to locate a pathogen, and the other nanomachine would be assigned to destroy it. So in order to accomplish a highly coordinated task, MC can be observed as an immediate and effective solution.

Due to the advent of nanotechnology, nowadays, it is possible to physically realize devices at nanoscale [52]. Therefore, these nanoscale based devices can further accomplish the complicated task of cooperation and communication via MC [53]. Further, these communicating nanodevices provide a significant enhancement in the early diagnosis as well as treatment of

various diseases and thus could revolutionize various aspects of biomedical engineering [54]. Nowadays, nanobots are employed for the transportation of molecular payload [55] and also for the discovery of brain aneurysm [56]. Similarly, various MC channel characteristic tools such as channel delay and path loss are utilized to analyze the pharmacokinetics of targeted drug delivery systems. In addition to this, the flagellated magnetotactic bacteria, along with MRI, can be utilized as a power nanobot for medical applications.

In contrast to the microscale applications, the MC systems at macroscale are employed in those environments where usually the basic EM wave-based communication systems fail to deliver promising results. For example, in some infrastructure monitoring environments, it can be observed that the present state of the art sensor network technology is not an entirely reliable means of communication [57]. Further, since EM wave-based communication in underground environments, such as oil-gas pipelines and underground mines, suffers from large diffraction loss and reliability issues, MC is a promising tool for communication in these environments. Moreover, MC can be used as a mathematical tool for modelling various environmental and animal activities. For example, animals, such as ants and bees, in nature rely on certain chemical signals known as pheromones in order to perform simple communication tasks [58]. Therefore, MC can be used to model this behaviour which would then be useful for future applications. Finally, inspired by pheromonal communication and olfaction present in nature, MC at macroscale also has a potential application in robotic search and rescue and robotic communication in strident environments.

1.1.7 Channel Models

The channel modelling corresponds to the theoretical modelling of the propagating media of any communication system. This theoretical modelling of any communication system can be accomplished by employing various information-theoretic concepts. Information-theoretic concepts are the mathematical foundations that are usually employed to analyze the characteristics of the channel, i.e., how a channel will behave towards a specific input. Compared to EM wave-based system where channel media varies from wired to wireless, in the MC scenario, the channel may vary from an aqueous medium without flow to a flow-based medium. The information molecule propagating through these channels majorly experiences noise, and this source of noise in MC can be expressed as a random propagation. Further, in the MC environment, the channel media plays a vital role in deciding the characteristic feature of the MC systems.

Therefore, different channel models can be mathematically obtained for different propagation and modulation techniques discussed in the previous sections. Particularly for a stable information channel having memory, the capacity is usually expressed as [6, eq. (24)]

$$C = \lim_{r\to\infty} \inf \sup_{x^r} I(\mathrm{X}^r; \mathrm{Y}^r), \tag{1.15}$$

where x^r is the sequence of r successive symbols that have been transmitted, and y^r is the sequence of r symbols that have been received at receiver correspondingly. In the case of diffusion-based systems, the channel model can be bifurcated into three major categories. The first is the models based on continuous diffusion equations, the second is the discrete models, and the third is the models having flow. Simultaneously, for different modulation schemes, the channel formulation can also be different.

In time-slotted binary-CSK (BCSK), where information propagation is achieved using a simple diffusion process, the channel can be expressed as a binary symmetric channel when ligand-receptors are employed for the detection process receiver. This type of modelling and analysis can be applied to relay channels as well as broadcast channels. Further, due to the random nature of the diffusion process, the MC channel also suffers from ISI. Therefore, to overcome ISI usually symbols with sufficiently large symbol duration is applied. Large symbol duration channel model corresponds to Markov chain where the transmit time of the present symbol is a combination of transmit time of present symbol and the transmit time of preceding symbol [59]. Additionally, for a ligand-based receptor channel, the capacity can be derived by modelling such systems as a Markov chain [60]. Moreover, the BCSK channel can also be expressed as a z-channel when there is no ISI, and for such a scenario, the information rates could be calculated via simulations [61]. Furthermore, for a generalized ISI model in z-channel MC, the system's noise can be modelled as Poisson-Binomial distribution. Using Poisson-Binomial distribution as a noise model, the maximization on the input probability distribution can be estimated according to [62].

In many practical environments, when the information molecules propagate, they experience a degradation phenomenon with time. For a BCSK channel, this molecular degradation process can be modelled as an exponential distribution. Based on the exponential distribution modelling, the channel capacity expressions for different degradation rates and modulation strategies can be calculated [63]. Correspondingly, for an energy-efficient end to end BCSK system, the maximization on the channel capacity can be achieved by employing an optimal

strategy for the transmission [64]. Another form of channel model with ligand receptors can also be employed in the MC environment where the solution to the diffusion equations is continuous. For these environments, the attenuation factor and delay functions can be calculated when the received signal is the convolution of transmitted signal and impulse signal with noise [65]. For the channels utilizing continuous diffusion, the solution to continuous diffusion equations can be calculated by averaging the system's behaviour for numerous trials. Further, instead of considering the continuous emission of the particles, it is desirable to consider the transmission of information particles to be a discrete number. The discrete nature of particles corresponds to quantization noise, and the random propagation of the diffusion process can be treated as an additive noise term. Therefore, the assumption of representing discrete nature of particles and random propagation as quantization and additive noise respectively helps in calculating the solution for the continuous diffusion equations [66]. Based on these calculations, the lower bound on the capacity of the MC in a vaporous environment can be obtained, and this capacity is a linear function of the bandwidth of the transmitted signal [67].

In the case of Microbial colonies, one of the prominent examples of practical MC environments, the mathematical models for the transmitter and receiver have been developed. The mathematical analysis shows that the system's capacity can be obtained when a reaction between the bacteria and the information molecules occurs. Further, the bacterial reaction produces a light and the luminance of this light increases as the reception concentration of information molecules increases at the receiver. Based on the reception power of the microbes, first, the optimal input distribution is obtained, and then this input distribution is used for the capacity calculations [68]. Similar to microbial colonies in case bacteria colony where the transmission is a two-tier process. In the first stage, the signalling or Type-A molecules are used to control Type-B molecules' emission. In the second stage, these Type-B released molecules arrive at the receiver via diffusion, which is recognized using ligand receptors. Therefore based on these observations, the channel capacity of the bacterial colony is obtained [69].

In the case of genetically modified cells, where the transmitter and receiver are genetically modified, the information can be conveyed via three-phased processes (collision, adhesion and neurospike transmission) [70]. Here, the transmitting and receiving cells undergo motion based on diffusion laws, and the process continues until both the cells undergo collision and adhesion, respectively. After collision and adhesion, the information transfer takes place with the help of a molecular neurospike. Based on these observations and some assumptions, the capacity of the

channel model is derived. Practically, the information molecules undergo chemical interactions with other molecules of the environment. Therefore, in order to model these channel environments, the reaction-diffusion master equation with exogenous input equations (RDMEX) are usually employed [71]. In order to analyze the changes in the channel, the RDMEX equations utilize the Markov model with discrete space and time. Meanwhile, the channel can be modelled using various stochastic models for the MC environment exhibiting particle absorption, generation and emission. Further, based on the stochastic modelling of the channel, the capacity expression for the diffusive environment with and without flow is obtained [72].

Generally, for on-chip applications, usually two configurations of kinesin molecules along with microtubule structures are used. In the first configuration, the mobile kinesin molecules move over a stationary microtubule, whereas in the second configuration scenario, the microtubule structure is mobile with stationary kinesin molecules. The first configuration scenario for transportation of information shows that the channel capacity of the kinesin-microtubule configuration is higher than the standard diffusion approach. Meanwhile, in order to calculate the channel capacity of the second configuration scenario, the use of the Markov chain provides accurate results [73]. Therefore, using Monte Carlo simulation, it can be observed that for MC environments where transmission of information over short distances is needed, the channel capacity of systems employing the diffusion process is higher than other modes of transportation. Whereas for MC environment where transmission of information over long distances is needed, then it is desirable to utilize flow based mechanism or active transport mechanism for molecular propagation in order to achieve higher channel capacity [74].

In the case of gap junctions where the transmitting nanomachine and receiving nanomachine are assumed to be artificial cell structures, the Ca^{+2} ions are used for information propagation. Specifically, in gap junctions, the Ca^{+2} ions propagate from one lattice structure to another until they arrive at their destination, where they are decoded for information. Therefore, for these channel models, the capacity expressions can be calculated based on the intercellular calcium wave model for different noise configurations as well as symbol duration [75]. A prominent example of a gap junction model is found in the cardiac muscles cells known as cardiomyocytes. In this environment, the channel capacity is calculated by modelling the regulated heartbeat [76]. On a similar ground, bacteria assisted propagation can be modelled using various mathematical expressions. Therefore, in order to represent any biological process mathematically, various communication theoretic channel models are utilized. For example, a harmonic transfer

matrix is used to model the flow of blood in blood vessels. In modelling of blood flow, a combination of two different models is used, wherein the first model considers smaller dimension arteries and the second model considers a relatively larger dimension for arteries [77]. For intercellular transduction channels with ligand receptors, the detection of information molecules at the receiver is characterized using the discrete-time Markov model. Another critical area where MC have a significant effect is in microfluidics. In a microfluidic environment, the channel modelling is accomplished by deriving the collective transfer functions of straight, turning, bifurcated and combinational channels [78].

Based on the aforementioned channel models, it is observed that for different MC environments, different channel models need to be employed. So in the following subsection, we will discuss the capacity formulation of DBMT channels where information encoding is done at the time of release and the propagation of molecules is achieved through diffusion.

1.2 Diffusion-Based Molecular Timing Channel and its Capacity

As discussed in the previous sections, one way to modulate information is at the time of release. Whenever the modulation of information is achieved via time of release rather than number or concentration, that channel is referred to as a timing channel. Therefore, the timing channel facilitates the accurate and meticulous analysis of the MC environments with stochastically independent arrivals of the information particles at the receiver. Practically, the sequences of DNA and protein molecules can be considered an example of a timing-based model for information transfer.

Moreover, MC is a cumulative approach that usually undermines physical phenomenons such as molecular emission and molecular reception of the information particles. Therefore, employing a concentration based technique for modulating information in MC environments may lead to certain fundamental limits in terms of capacity formulation. So in order to overcome the practical limitations of the concentration based modulation, timing based channel models are usually employed. Compared to the concentration-based modulation technique, the timing-based channels ensure molecular arrival at the receiver, ensuring reliable information transmission. In the timing channel, the tokens (also known as information particles) used do not undergo modification or alteration, and the difference only occurs in the molecular release

and arrival times at the transmitter and receiver, respectively. However, due to some parallel processes co-occurring in the MC environment, it is appropriate to consider that the information molecules (tokens) get lost and never arrive at the receiver. In concentration based modulation techniques, the lost molecules cause severe ISI problems, which leads to lower channel rates. However, in timing channels, due to the presence of time slots for communication, the molecules lost in the environment are destroyed, and therefore they do not create the ISI problem. Meanwhile, the timing based model can also be employed in the MC environments where there is a need for re-sequencing of the information particles at the receiver. In case of transmission of a large number of information molecules, the timing channels provide tight bounds on the re-sequencing of the information molecules at the receiver. The analysis of timing channels usually provides upper and lower bounds on the channel capacity, and this capacity formulation can be accomplished by taking into consideration various cascaded models of the timing channels. One such example of employing the timing channel is in the channel models where information carriers are transmitted during signalling intervals.

Once released in the fluid medium, an information molecule takes a random path and propagates through diffusion before reaching the receiver. This type of model where information is in time of release and propagation mechanism is diffusive is known as diffusion-based molecular timing (DBMT) channels. The DBMT channels are the most energy-efficient means of communication at the microscale level. In MC environments, the symbol duration usually affects the diffusive propagation mechanism of the system. The changes in the symbol duration subsequently affect the channel capacity of the system. Therefore, defining the channel capacity in capacity per channel usage rather than bits per second becomes imperative. Typically, the term bits are usually used to characterize information transfer in EM wave-based communication systems. However, in the MC environments, the information is encapsulated in the biological phenomena occurring in nature; therefore, alphabets instead of bits are used to depict information. For example, the proteins alphabet is usually composed of 20 natural amino acids in biological environments, whereas the DNA alphabet is composed of 4 natural nucleotides. Therefore, due to the arbitrary nature of bits, it is desirable to use bits to represent the information content of alphabets in terms of bits [79]. In DBMT 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

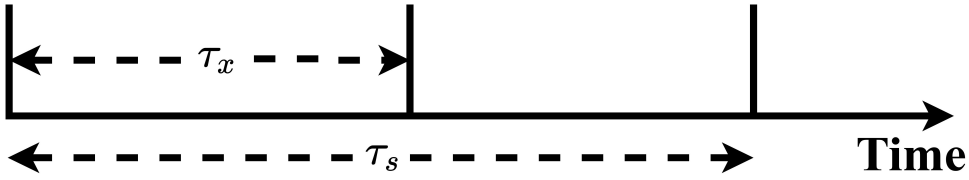

Figure 1.2: Timing diagram of molecular timing channels [80].

term is characterized by inverse Gaussian (IG) [17]. For a drift-free environment, this noise term follows a Lévy distribution [80]. Unlike the IG distribution with exponentially decaying tails, the Lévy distribution is α-stable having algebraic tails [81]. The stability of a Lévy distributed random variable (RV) 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 [82]. A more detailed mathematical expression of truncated Lévy distribution will be discussed in the subsequent chapters.

1.2.1 Timing Channel Capacity Formulation

In timing-based MC systems, the transmitter is usually assumed to be a point source capable of emitting information particles in large numbers. The transmitter perfectly controls the time of the release of molecules, and the receiver measures the arrival times perfectly. Moreover, all the information particles released in the media follow independent paths. The time the information molecules take to reach their destination is random and is denoted as random propagation delay. The random propagation delay behaves as an additive noise term which is represented by truncated Lévy distribution. Further, the DBMT channel is divided into time slots (τ_s). The time slot τ_s, is mathematically expressed as $\tau_s = \tau_x + \tau_m$, where τ_x represents the symbol interval in which the transmission takes place at a particular time instant and τ_m is the time taken by the information molecules to decay to $X\%$ of its initial value. Figure 1.2 depicts the pictorial representation the slot duration τ_s employed in the DBMT channels. Similarly the block diagram representation of a general DBMT channel is shown in Figure 1.3. From the figure, it is observed that the timing channel comprises two-channel model scenarios. The information is decoded at the receiver in the first scenario whenever the random propagation delay is less than the particle's lifetime. Meanwhile, no information is decoded at the receiver in the second scenario when the random propagation delay is more than the particle lifetime. The transmission time in the ith transmission slot is given as $T_{t,i}$. Let $T_{a,i}$ represents the arrival time of the

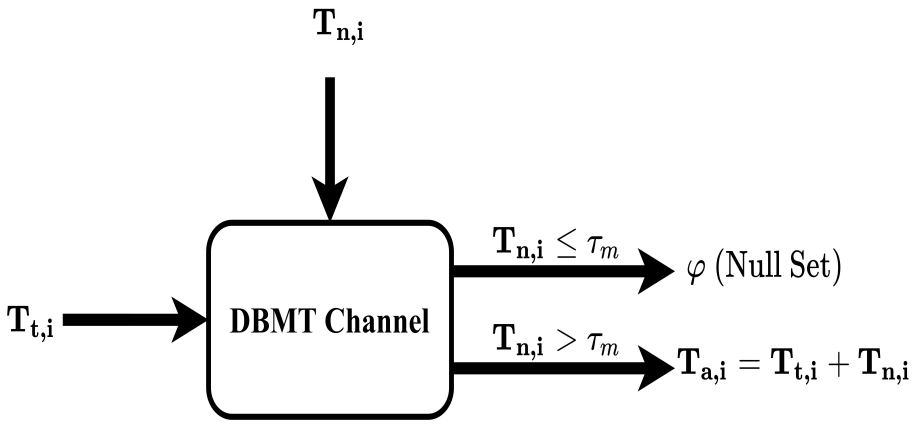

Figure 1.3: General block diagram of molecular timing channels [83].

molecules at the receiver. Therefore the arrival time is expressed as

$$O_i = \begin{cases} T_{a,i} = T_{t,i} + T_{n,i}, & \text{for} \quad T_{n,i} \leq \tau_m \\ \varphi & \text{for} \quad T_{n,i} > \tau_m, \end{cases} \tag{1.16}$$

where O_i is the channel output of the DBMT channel considering both scenarios and $T_{n,i}$ is random propagation delay. Further, the transmit time of the molecules follows

$$(i-1)\tau_s \leq T_{t,i} \leq (i-1)\tau_s + \tau_x. \tag{1.17}$$

Let $\mathscr{E}_i \triangleq [(i-1)\tau_s, (i-1)\tau_s + \tau_x]$ and $\mathscr{D}_i \triangleq \{[(i-1)\tau_s, i\tau_s] \cup \varphi\}$ for $i = 1, 2, ..., P$. Therefore, for the molecular timing channels the code is expressed as (P, R_a, τ_x, τ_m), where P is the code length and R_a code rate. In molecular timing channels, the message set is given as $\mathscr{I} = 1, 2, ..., 2^{P(\tau_s)R_a}$, an encoding function is represented as $\varepsilon^{(P)} : \mathscr{I} \mapsto \mathscr{E}_1 \times \mathscr{E}_2 \times \cdots \times \mathscr{E}_P$ and decoding function is defined as $\nu^{(P)} : \mathscr{D}_1 \times \mathscr{D}_2 \times \cdots \times \mathscr{D}_P \mapsto \mathscr{I}$. Since the timing channel considered is similar to that considered in [83]; therefore the codebook size becomes a function of τ_s with $P(\tau_s)$ representing the maximum time taken for the transmission of information using (P, R_a, τ_x, τ_m) code. Further, the encoder maps the information $I \in \mathscr{I}$ into L time indices, where $T_{t,i} \in \mathscr{E}_i$ for $i = 1, 2, ..., P$. After passing through the DBMT channel the encoded transmitted information reaches the receiver where the information decoding is done by utilizing channel outputs O_i where $O_i \in \mathscr{D}_L$.

The capacity analysis is done on per time slot basis therefore for the sake of simplicity it is appropriate to drop i term from $T_{t,i}$, $T_{a,i}$ and $T_{n,i}$. Since T_n is independent of T_t, so the channel

capacity per time slot is given as [83, eq. (7)]

$$C = \max_{\tau_x, \mathscr{F}(\tau_x)} \frac{I(T_t; T_a | T_n \leq \tau_m) F_{T_n}(\tau_m)}{\tau_s} = \max_{\tau_x, f_{T_t}(t_t)} \frac{h(T_a | T_n \leq \tau_m) - h(T_n | T_n \leq \tau_m)}{\tau_s}, \tag{1.18}$$

where $\mathscr{F}(\tau_x)$ denotes the set of all p.d.fs, $F_{T_n}(\tau_m)$ represents the CDF of T_n, $I(;)$ denotes mutual information and $h(.)$ represents the differential entropy, with maximization simultaneously done over τ_x and the distribution for T_t. Since it is difficult to calculate the exact expression of capacity as the maximization on input distribution $f_{T_t}(t_t) \in \mathscr{F}(\tau_x)$ is difficult to obtain analytically. Therefore, we rely on the upper and lower bounds on the capacity.

1.2.1.1 Single-Particle DBMT channel

In the case of a single-particle DBMT channel, the transmitter emits a single-particle in each time slot. Let R be a Bernoulli random variable (RV) where $R = 1$ representing the scenario when the molecule is received at the receiver within a time slot, with p_τ as the reception probability. Therefore, in a time slot there are two probabilistic scenarios, the first scenario being given as $\mathbb{P}(R = 1)$=p_τ which represent molecular hitting probability and the second scenario being represented as $\mathbb{P}(R = 0)$=$1 - p_\tau$. The hitting probability of the molecule is expressed as [82, eq.(32)]

$$p_\tau = \mathrm{e}^{\sqrt{2c\alpha}} \sqrt{\frac{c}{2\pi}} \left(2\sqrt{\frac{p}{c}} K_{1/2}(p) - \sqrt{\frac{1}{\tau_m}} K_{1/2}\left(\alpha\tau_m, \frac{c}{2\tau_m} \right) \right), \tag{1.19}$$

where $c = d^2/2D$ is Lévy noise parameter, α is degradation parameter, $K_{1/2}(p)$ is the modified Bessels function of second kind, $K_{1/2}\left(\alpha\tau_m, \frac{c}{2\tau_m}\right)$ is the incomplete Bessels function and $p = \sqrt{2c\alpha}$ is the scaled version of the Lévy noise parameter. Therefore, using this expression the upper and lower bound on the capacity is given as

$$C_{ub} = \max_{\tau_x} \frac{p_\tau}{\ln(2)} \left\{ \frac{\ln(\tau_s) - h(T_n | R = 1)}{\tau_s} \right\}, \tag{1.20}$$

$$C_{lb} = \max_{\tau_x} \frac{p_\tau}{\ln(2)} \left\{ \frac{\ln\left(2^{2\ln(\tau_x)} + 2^{2h(T_n|R=1)}\right) - 2\ln(2) h(T_n | R = 1)}{2\ln(2)(\tau_s)} \right\}, \tag{1.21}$$

where $\ln(.)$ denotes natural logarithmic function.

1.2.1.2 Multi-Particle DBMT channel

In case of multi-particle DBMT channel the transmitter emits N identical information particles in each time slot. The release of information molecules or particles is instantaneous and the number of molecules is same for all the input messages. For a multi-particle DBMT channel the expression (1.16) is modified as

$$T_{a,j} = T_{t,j} + T_{n,j}, \tag{1.22}$$

where $T_{a,j}$ for $j = 1,2,3,...,N$ corresponds to the arrival time of the jth arrival. Let M represent the number of molecules that arrive at the receiver within a time slot such that $M \in ,1,2,3,...,N$. Since the path taken by all the molecules are independent and identically distributed, then the capacity of the channel is represented by the number of molecules that arrive at the receiver only. Thus the mathematical expression of (1.22) becomes

$$\mathbf{T_a} = \mathbf{T_t} + \mathbf{T_n}, \tag{1.23}$$

where $\mathbf{T_a}$, $\mathbf{T_t}$ and $\mathbf{T_n}$ represents vectors of length M. Based on these observations the mutual information for a multi-particle can be mathematically expressed as

$$I(\mathbf{T_t};\mathbf{T_a}) = \sum_{m=1}^{N} P(N,M=m) I(\mathbf{T_t};\mathbf{T_a}|M=m), \tag{1.24}$$

where $I(\mathbf{T_t};\mathbf{T_a}|M=m) = h(\mathbf{T_y}|M=m) - h(\mathbf{T_n}|M=m)$ and $P(N,M=m)$ is the binomial distribution with N and p_τ being its parameters. Moreover, the binomial distribution with N and p_τ its parameters is basically the summation of N independent and identical distributed Bernoulli trials. Thus using this notion the mutual information expression in (1.24) is modified to

$$I(\mathbf{T_t};\mathbf{T_a}) = N p_\tau \left(h(T_y|R=1) - h(T_n|R=1)\right). \tag{1.25}$$

Since the mutual information of the multi-particle system obtained in (1.25) is N times the mutual information of a single-particle. Therefore, the expression of C_{ub} and C_{lb} for a multi-particle system becomes N times that of a single-particle system.

Let the number of molecules emitted by the transmitter is large enough such that $M \geq N_c$ where N_c is the cross-over number from Lévy to Gaussian regime. Based on this, for the case of

large N, the receiver applies a linear averaging filter. Therefore, $M = Np_\tau$ signifies the average number of molecules that arrive within a time slot. For such a system, the capacity upper and lower bounds are expressed as

$$C_{ub}^{G} = \max_{\tau_x} \frac{2\ln(\tau_s) - \ln(2\pi e/M^2\alpha^2)}{2\ln(2)(\tau_s)}, \tag{1.26}$$

$$C_{lb}^{G} = \max_{\tau_x} \frac{1}{2\ln(2)(\tau_s)} \left\{ \frac{1}{\ln(2)} \ln\left(2^{2\ln(\tau_x)} + 2^{2\ln\left(\frac{2\pi e}{M^2\alpha^2}\right) - \ln\left(\frac{2\pi e}{M^2\alpha^2}\right)} \right) \right\}. \tag{1.27}$$

Practically, the timing-based modulation is observed inside the synaptic cleft of the human brain [83]. 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 [67]. 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 [15]. Thus the concept of secure transmission becomes imperative to be used in this relatively new field of communication since there is a propagation of privacy-sensitive information from the transmitter to the receiver [84]. Therefore, in the next section, we will discuss the main motivation of analyzing the DBMT from the secrecy perspective.

1.3 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. Based on the existing 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 significant limitations. As is the case with any communication system, the secure transmission of information from Alice to Bob without any interference from Eve is highly desirable. For example, in the case of the targeted delivery of drug molecules to a malignant tumour node. Here, it is to be ensured that the drug is delivered to the concerned node only and not to the adjacent healthy nodes to avoid any side effects and minimize any drug wastage. In this case, the adjacent healthy node might act as a predator receiver that tries to attract drug molecules intended for the malignant node. Thus, it becomes imperative for the system to have robustness in terms of secure information transfer, especially in healthcare applications.

Furthermore, with the inability of the molecules to distinguish between the two receivers (either Bob or Eve), it becomes imperative to analyze the system's robustness in terms of secrecy whenever the predator receiver tries to retrieve sensitive information. In MC, there are 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 reach the legitimate node; thus usage of secrecy for information transfer becomes vital.

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. Additionally, the elemental study of secure communication at the early stage of molecular communication is easier than the analysis done after a considerable headway has been accomplished in this promising technology. Moreover, in many practical applications, the instantaneous channel state information (CSI) of eavesdropper (Eve) is not known at Alice, so the need for secrecy to ensure uninterrupted information transfer becomes essential. Despite the vital role of secrecy in MC, there is a dearth of research in this field. The MC system under consideration comprises Alice, Bob, and Eve wherein the exact distance or the exact number of molecules at the eavesdropper from the legitimate source is unknown. However, in some practical scenarios, there is some knowledge about the behaviour of Eve and this prerequisite knowledge is denoted in terms of first and second moments, i.e., in terms of mean and variance. These moments are usually obtained by employing maximum likelihood estimation by observing the sampled observations. The maximum likelihood estimation is based on the joint probability density function of the received samples at the receiver. Therefore the development of analysis related to security with the help of various secrecy performance metrics would then be helpful to attain secrecy in the MC systems.

1.4 Research objectives

In the thesis, the secrecy performance of the diffusive molecular timing channel is being analyzed. In this context, various secrecy performance metrics are being used to analyze and validate the effect of eavesdropper in the DBMT channels.

1. To calculate the upper bound on the average eavesdropper capacity of a single-particle diffusive molecular timing channels when the distance of eavesdropper is assumed to be uniform and Gaussian distributed.

2. To analyze the effect of eavesdropper by calculating the expressions of various secrecy performance metrics (Generalized Secrecy Outage Probability, Average Fractional Equivocation, Average Information Leakage Rate) for single-particle diffusive molecular timing channels in the partial secrecy regime by employing the concept of fractional equivocation.

3. To optimize various secrecy performance metrics in order to calculate the optimal rate parameters. Further, calculating the optimal rates which would minimize generalized secrecy outage probability, maximize average fractional equivocation and minimize average information leakage rate of the diffusive molecular timing channels.

4. To analyze the amount of confusion level for the multi-particle DBMT channels by taking into consideration the expressions of generalized secrecy outage and average fractional equivocation.

5. Finally, to examine the amount of secrecy loss in the multi-particle diffusive molecular timing channels. The secrecy loss metric uses a unified second-order metric that quantifies the severity of confidential information leaked towards Eve in the DBMT channels.

Based on the objectives mentioned above, the following is the list of the work accomplished during the thesis work. The objectives completed till date are given as:

- We have obtained the expression of average eavesdropper capacity when the distance of eavesdropper is uniform and Gaussian distributed.
- We have analyzed the secrecy performance of the DBMT channels for single-particle and multi-particle scenarios. We employed various secrecy metrics for the analysis, such as GSOP, Average fractional equivocation and Average information leakage rate.
- To obtain valuable insights, we compared our analytical results with the generalized expressions for the outage probability available in the literature.

- We validated various secrecy performance metrics by comparing the analytical results of the above-mentioned secrecy performance metrics with simulation results obtained by undertaking particle-based simulations.

- We have obtained the optimal secrecy and transmission rate of Bob transmission rate. These optimal calculated rates would then help minimize GSOP, maximizing average fractional equivocation and minimizing average information leakage rate (R_L) in a DBMT channel.

- We have proposed a new secrecy metric, namely amount of confusion level, which considers second-order statistics. The amount of confusion level metric is a helpful secrecy measure that gives information about the level at which Eve is confused.

- Finally, we also examined the secrecy of the DBMT channel from the secrecy loss perspective. The secrecy loss metric shows the severity of information loss in the DBMT channels.

1.5 Thesis outline

The subject matter of the thesis is presented in the following five chapters,

- Chapter-1 gives an overview of molecular communication. Mainly diffusion-based process and the diffusion-based molecular timing channels. It also describes an outline of the various modulation techniques in MC and emphasizes the motivation of this research along with the research objectives.

- Chapter-2 provides a survey on molecular communication from the perspective of communication engineering. In particular, an overview of molecular timing channels is presented, followed by a detailed review of capacity and secrecy analysis in molecular communication.

- Chapter 3 describes the secrecy performance analysis of single-particle DBMT channels when the distance of the eavesdropper is considered to exhibit Uniform and Gaussian distribution. Specifically, a detailed capacity analysis is presented in the chapter wherein an upper bound on the average eavesdropper capacity is calculated in uniform and Gaussian

regimes. Moreover, the secrecy analysis from the partial secrecy regime perspective is also included in the chapter.

- Chapter-4 discusses the design aspect of the DBMT channel from the secrecy perspective. Notably, in the chapter, the optimal rate parameters which would minimize generalized secrecy outage probability, maximize average fractional equivocation and minimize average information leakage rate is studied. Further, the system's optimization analysis emphasized that for particular optimal rate parameter values, there is always a trade-off between various secrecy performance metrics.

- Chapter-5 highlights the secrecy performance of the multi-particle diffusive molecular timing channels from the amount of confusion level perspective. In particular, a new secrecy metric for the molecular timing channel is proposed. This new secrecy metric, namely the amount of confusion level, is based on the second-order statistics of the fractional equivocation. In addition to the new secrecy metric in this chapter, other existing secrecy performance metrics are also analyzed for the multi-particle system.

- In Chapter-6, the secrecy loss for multi-particle diffusive molecular timing channels is studied. Assuming the distribution of the received molecules at Eve to be Gaussian distributed, we calculate the secrecy outage probability and average secrecy rate of the diffusive molecular timing channels. Subsequently, we calculate the amount of secrecy loss using the secrecy outage and average secrecy rate expressions.

- Finally, in Chapter-7, the secrecy analysis of the DBMT channels using different secrecy metrics are summarized. The future scopes of the research works are proposed successively, following the conclusion based on substantial extracts and understanding of the subject of interest.

Chapter 2

Review of Literature

As discussed in the previous chapter, the aspects of secrecy in MC is one of the most challenging areas as it has potential applications in biological fields such as human healthcare, environmental safety and various forms of bioterrorism. Therefore, it becomes imperative to study the secrecy performance of MC systems, especially the systems employing diffusive molecular timing channels. Keeping these aspects in mind, various researchers around the globe have studied both the molecular timing channels and secrecy aspects of MC systems separately. In this chapter, a brief review of MC, information-theoretic capacity in MC, molecular timing channels and secrecy in MC systems have been described, respectively.

2.1 Overview of Molecular Communication

The famous speech: 'There is Plenty of Room at the Bottom' [85] given by the Nobel laureate Richard Feynman on 29^{th} December 1959 at the American Physical Society meeting in Caltech laid the foundation of nanotechnology. The primary objective of the speech was to encourage the legion of researchers to find the solution to the problem of manipulating and controlling things on a micro or nanoscale level. Since then, there have been significant advancements in nanotechnology in the past few decades. With the advent of new research fields such as micro-electro-mechanical systems (MEMS) and nano-electro-mechanical systems (NEMS), the design of microscale or nanoscale devices is now very much possible. In addition, the coordination of these devices to accomplish a highly sophisticated and complicated task requires the formation of multiple nanoscale networks (typically known as nano-networks). Therefore, the formation of nanonetworks requires the miniaturization of current existing communication systems. The

current EM wave-based communication systems heavily rely on the EM spectrum. However, curtailing the current EM wave-based communication system to a nanoscale dimension is a challenging task as it requires reducing the size of the transmitter and receiver to nanoscale levels. Therefore, various alternative means of communication, especially MC, is being used to overcome the aforementioned challenge. MC is one of the oldest existing technologies, which is prevalent in various naturally occurring phenomena. In nature, various microorganisms such as cells and bacteria gain information from their environment by exchanging chemical signals. The transmission of information in the form of information molecules was first discussed by [86]. In the paper, the authors majorly focused on the design of diffusion-based MC systems. Since then, the work on MC has only accelerated. In MC, the different techniques that are used for the transfer of information molecules from transmitting nanodevice to a receiving nanodevice are diffusion-based, active transport based, bacteria-based and flow-based. Diffusion-based MC was first analyzed by [87, 88, 89], in which the authors collectively discussed the transmission of information from transmitting nanomachine to a receiving nanomachine by undergoing Brownian motion. In diffusion-based MC, the molecules travel a significant distance from the transmitting nanodevice to the receiving nanodevice by undergoing random walks in the environment. In other molecular propagation approaches, such as flow-based or advection-based, the molecular propagation from transmitter to the receiver is accomplished via molecular motors or biologically engineered bacteria.

In an advection or flow-based mechanism, the information molecules propagate through diffusion in a fluidic medium whose flow or advection mechanism is defined and predictable. One of the examples where gap junctions were used as a mode of transportation of information molecules was analyzed in [90]. The authors in [90] utilized nanofluidic pipes for connecting the transmitter and the receiver. Flow-based transportation mechanism can also be implemented by using carrier particles whose motion, despite being random, is constrained on the average along the dedicated path. Another good example where a flow-based approach is used is the chemotaxis-based technique. The authors in [91, 92] highlighted the use of advection- or flow-based mechanism. The authors, in their work, utilized flagellated bacteria for the propagation of information encoded DNA molecules from the transmitter to the receiver, and these information encoded DNA molecules propagating towards the destination are subsequently attracted and decoded for information.

Another mode of transportation in MC is the walkway-based MC, in which the transporta-

tion of information molecules by active propagation is executed by following a pre-defined path connected from the transmitter to the receiver. This type of transportation mechanism in MC literature is accomplished by the use of molecular motors [93, 94]. The authors in [93, 94] studied molecular motors filaments and used these filaments to interconnect nanomachines physically. These interconnected nanomachines are therefore used to generate the force which is responsible for information transfer. Molecular motors, as indicated by authors in [95] are the protein filaments that convert chemical energy into kinetic energy. These protein filaments are basically the main reason for generating force in biology, especially in muscles. Out of all the modes of propagation, the most widely employed mechanism is the diffusion-based approach. This is primarily because, compared to the other modes of transportation, the diffusion process remains at the core level of molecular propagation, and it is also the most general and standard MC transportation mechanism option in nature.

Many diffusion-based MC systems have been highlighted and studied in the MC literature, and these have further been used for the physical and analytical implementation of nano-networks. Subsequently, different diffusion-based MC architectures have been classified based on different information molecules encoding techniques. In MC literature, different properties of the information molecules in many diffusion-based MC systems have been highlighted and studied. These properties have further been used for the physical as well as the analytical implementation of nano-networks. Subsequently, different diffusion-based MC architectures have been classified based on different information molecules encoding techniques. In MC, various characteristic features of the information molecules are used to encode the information. The information encoding is based on the time of release of the information molecule, the type of molecule (DNA or RNA molecule), the position of the molecule and the number of molecules released by the transmitter. The MC architecture where the encoding of information was in the time of release was theoretically analyzed in [96]. In [96] the authors primarily focused on the mathematical modelling of the diffusion-based molecular channel as a probabilistic contribution in the time of arrival of the molecules at the receiver. While the authors of [96] used time of release as an encoding method, the authors in [94] used the type of molecule mechanism for encoding information. In [94] authors used a certain type of molecule for the transmission of information from the transmitter to the receiver. Therefore, the information is only received in this approach if the receiver receives a particular type of molecule transmitted by the transmitter.

2.2 Information Theoretic Capacity in MC

The primary objective of any communication scenario is the transmission of information from the transmitting side to the receiving side without significant loss of information [97]. In order to accomplish such a daunting task, EM wave-based signals are primarily used. However, at the nanoscale level, MC has found its application and is emerging as a potential candidate for the information propagation [6]. Despite the applications of MC in nanoscale communication, there are still certain aspects, especially in terms of information-theoretic capacity, that needs to be addressed. The author in [23] and [98] was the first one to estimate the achievable information-theoretic rate in MC scenario using Brownian motion of the information molecules. In [23] the author proposed various mathematical models as well as techniques for the calculation of channel capacity in the timing based channels. The author showed that under certain assumptions, the channel capacity of the timing channel surpasses 1-bit per particle. Compared to an identical, indistinguishable set of information molecules used in [23], the author in [98] utilized a different set of information molecules in order to achieve a good information rate. The author also proposed that optimal input distributions, as well as optimal approximations, are needed in order to attain maximum achievable channel capacity. Meanwhile, the authors in [89] developed an information-theoretic model to analyze the molecular channel capacity among two nanomachines. The authors in [89], utilized the laws of mass-action to derive the closed-form expression of channel capacity between a transmitting nanomachine and a receiving nanomachine. Further, they also observed that the maximum achievable capacity is obtained by changing the physical parameters of the environment. In [99] and [94] the authors explored different MC propagation media in order to characterize the information-theoretic capacity of MC channels. Basically, two types of MC systems, namely unicast and broadcast, were studied by the authors. The authors analyzed the information rate between a single transmitter and a single receiver in the unicast-based MC system based on different propagation mechanisms. Compared to various conventional propagation mechanisms, the information rate in the case of unicast MC systems was higher. However, in the broadcast scenario, the propagation mechanism choice does not significantly affect the information-theoretic capacity. Moreover, the noise models in the unicast mode were considerable while using hybrid aster as a propagating mechanism, whereas for the broadcast mode, the noise models were critical for all the propagating mechanisms under consideration. Meanwhile, the author in [100] tried to relate the

natural heredity process occurring in nature as an encoded communication phenomenon. In [91] the authors proposed a MC network architecture for medium-range MC scenario. Further, the authors also proposed catalytic nanomotors and flagellated bacteria as new propagation mechanisms for medium-range MC systems. Simultaneously, the authors in [101] experimentally investigated the channel capacity of Ca^{+2} signalling molecules in a molecular relay channel. The authors from their numerical analysis suggested that the maximization of the information-theoretic channel capacity can be accomplished by varying the transmitter and receiver numbers and altering the channel's characteristic features.

An analogous iterative model for the protein-based systems useful for relating the evolutionary process was proposed by the authors in [102]. The authors in [102] calculated the information-theoretic capacity bounds of the protein-based communication channel. Further, the authors also computed the rate-distortion functions for archaea, bacteria and eukaryotes, which are the three basic entities of any living organism. Finally, based on the numerical analysis, the authors drew significant insights into the evolutionary process dynamics. Simultaneously, in [103] the authors provided an information-theoretic model for diffusion-based MC systems. The authors employed two different approaches for modelling noise mathematically. In the first approach, the system's noise is modelled via ligand-receptor kinetics, whereas in the second approach, the noise was modelled using stochastic chemical kinetics. Further, the authors derived the closed-form expression of reception noise at the receiver from the stochastic chemical kinetics model. In [59] and [60] the authors developed an information-theoretic capacity expression for the time-slotted MC systems with information in the concentration of molecules. Moreover, the authors in both papers proposed achievable capacity rates by modelling the diffusive channel with memory as a two-step Markov chain. The capacity expressions derived in [59] and [60] were based on the mutual information between the transmitted number of particles and the number of particles arriving at the receiver. However, in [43] authors proposed a new scheme known as MARCO based on transmission order of distinct molecules. The authors first analyzed the proposed model in terms of error probability, and then based on error probability analysis, feasible information-theoretic rates were obtained analytically. Simultaneously, in [17] the authors provided lower and upper bounds on the channel capacity for the AIGN channel where the information was in the time of release. Similarly, by utilizing the same constraints, the author in [104] derived a different set of bound on the capacity for the AIGN channel. Further, the authors in [105] tightened the capacity bounds derived by au-

thors in [17] and [104] by characterizing the input distribution. Likewise, in [106] the authors used a different constraint for limiting the maximum arrival time of the particle and based on this, an upper bound on the channel capacity was presented. In [107], authors used Shannon's information-theoretic concepts to find the capacity of cellular signalling channels. They showed that channel capacity becomes zero whenever the biochemical system's free energy expenditure becomes zero. Moreover, they also observed a positive correlation between channel capacity and free energy expenditure.

Authors in [74] examined confined space MC systems in order to compare the achievable information-theoretic capacity of active transport MC systems with that obtained in the case of passive transport. The authors also observed that the information rate of the system increases by altering the shape of the transmission area. Similarly, the authors in [108] presented a mathematical expression for the transmission probability that maximizes the information-theoretic capacity of the MC system. The authors further noticed that the wandering molecules in the MC environment negatively affect the system's performance. Likewise, a concentration based MC channel capacity expression with molecular degradation was obtained by authors in [109]. Simultaneously, in [67] the authors analyzed the concentration modulated MC channel and provided a closed-form capacity expression in terms of diffusion coefficient, transmitter and receiver distance, transmitted signal bandwidth and average thermodynamic transmitted power. Further, in order to give a more practical aspect to information-theoretic analysis in biology, the authors in [110] calculated Shannon's information-theoretic capacity of DNA sequences modelled using the Kimura model. Additionally, in order to increase reliability while keeping decoding complexity lower, the authors in [111] provided ISI free channel codes for the diffusive MC channels. Subsequently, authors in [44] proposed a new modulation scheme for MC, which exceeds the in terms of error performance when compared with the existing modulation schemes. Furthermore, the importance of persistence length in the modelling, as well as simulation of nanonetworks, was highlighted by authors in [112]. The authors investigated the essential properties of nanonetworks by taking into consideration various filamentous structures. The use of enzymes for the creation of an ISI free diffusive MC system was undertaken by authors in [113]. The authors employed enzymes to attain intermediate reaction with the information molecules so that the information molecules do not cause ISI. Subsequently, the error performance of the system was presented.

The authors in [73] used a Markov chain to model the active transport MC channel where

molecular motors were used for the propagation of information particles. Using the Markov chain model, the authors further derived the channel capacity of the active transport MC channel. The authors in [114] used various information-theoretic metrics for the detection of deformity in the cellular tissue. The authors employed a classifier and various information-theoretic concepts and detected the deformation type, the deformation level, and the distances between the deformation and the nanomachine. Furthermore, the authors in [115] modelled and evaluated the uncertainty in the human cardiovascular system due to noise from the information-theoretic perspective. The authors derived the capacity of the particle drug delivery system by considering all the noises and physical constraints present in the environment. Correspondingly, the authors in [116] presented capacity analysis for the microfluidic environment while considering interference. The authors analyzed the information-theoretic capacity of the system while considering three different interference (microfluidic both sided interference, microfluidic single-sided interference and microfluidic interference-free) configurations. Meanwhile, the authors in [117] calculated the information-theoretic channel capacity of bacterial cables where the propagation is through electrons. The authors also considered the case where the CSI of the channel is available at encoder and decoder. Subsequently, they analyzed the discrete version of the continuous system by considering the fact that the capacity of finite-state Markov channels is known.

Correspondingly, the authors in [118] provided an information-theoretic capacity for a Ca^{+2} signalling based MC systems in a biological tissue environment. Accordingly, the authors in [119] proposed a novel information-theoretic model for interpreting nonlinear, time-varying communication channels comprising of stimulus generation, brain processing and response measurements. The authors used information-theoretic measures (mutual information) to analyze the quality of the audio signal generated from brainwaves in the presence of time-varying distortions. Additionally, authors in [120] studied the information-theoretic capacity of MC in a fluidic medium. The authors obtained upper and lower bounds on the capacity in two scenarios. In the first case, they assumed that the ISI was negligible, for which they calculated the information-theoretic capacity, and subsequently, in the second case, the bounds on the capacity were calculated when the system suffers from ISI.

In [121] the authors proposed a multiple input multiple output MC environment where ISI is prevalent. The authors considered detection algorithms for four symbols which is mainly dependent on the information received at the receiver. Based on this, the information rate of

the system was analyzed. Simultaneously, authors in [122] presented a trade-off between information rate and error probability for diffusive MC channels where information is in the binary concentration of molecules. In addition to [122], the authors in [123] modelled biochemical signal transduction as a discrete-time finite-state Markov channel. For this Markov channel, the authors obtained information-theoretic capacity by considering the input distribution to be iid. Further, they demonstrated that the discrete-time channel capacity approaches the Kabanov-Poisson channel capacity for short time steps. Likewise, in [124] the authors used the concept of rate-distortion theory to evaluate the capacity of biological signalling pathways where due to environmental noise, error-free communication is not possible. Meanwhile, the authors in [125] derived the information-theoretic capacity of the quantum-based biological channel using phonons as the information molecules. Besides, the authors in [8] highlighted various information-theoretic concepts that can be utilized in MC to attain achievable channel capacities. Likewise, an information-theoretic viewpoint on the palimpsests in the case of neural memory was illustrated by authors in [126]. Simultaneously, authors in [127] presented a closed-form expression for the channel capacity in multi-layer diffusive MC channels. The authors obtained the capacity expression for molecular transmission via air-water blood plasma channel depicting the process of multi-layer diffusion inside the respiratory system.

The authors in [128], and [129] provided the capacity bounds for the inscribed matter communication channel where the information particles are considered to be indistinguishable. The authors calculated the capacity bounds of these channels by considering that all the information molecules transmitted by the transmitter arrive at the receiver eventually, with the first arrival time being finite. On the contrary, the authors in [130] calculated the information-theoretic rate for the generalized inverse Gaussian diffusive model of the cortical neurons. Here the authors examined the mutual information of the system for fixed average energy. The authors in [131] studied the maximum achievable information rates for MC channels employing ISI avoiding modulations wherein practically long blocklength codes and delays are required to attain desired coding capacity. However, the authors in their paper considered shorter blocklength codes at the decoder to reduce complexity without compromising on the given constraints of the system. Meanwhile, in [132] authors derived the upper as well as lower bounds on the capacity of the α-stable noise channels. Further, the bounds were compared with the numerical approximations obtained through the Blahut-Arimoto algorithm to obtain more useful insights into the system. The authors studied an information-theoretic model for the insulin-glucose system

in [133]. The authors used insulin and glucose molecules for carrying information and subsequently analyzed the system in terms of channel capacity and channel propagation delays. Meanwhile, the authors studied the physical limit on the capacity for broadcast MC microfluidic channel in [134]. The authors used Fick's laws along with Shannon's information-theoretic capacity to indicate the impact of molecular propagation on the channel's capacity. Additionally, the authors in [135] used the z-channel model for calculating the capacity of the molecular optical channel model, which is based on the phonon energy transfer mechanism.

The capacity lower and upper bounds of additive signal-dependent noise channels were highlighted by authors in [136]. The authors proposed that decreasing noise variance does not increase the capacity of the additive signal-dependent noise channels. Meanwhile, a novel DNA-based MC protocol was presented by the authors in [137]. Based on the proposed model, high channel capacity between the nanomachines was obtained. Further, the authors in [138] derived an achievable information rate in flow-based diffusive MC channels. Similarly, an information-theoretic capacity of energy-efficient hierarchical nano-communication networks at THz frequency was calculated by authors in [139]. Parallelly, the authors in [140] computed mutual information for two different receiver configurations (series and parallel). Further, the authors also calculated the achievable information rates for single action potential signals. Likewise, an information-theoretic analysis to quantify Ca^{+2} signalling was proposed by authors in [141]. The authors utilized mutual information metric for measuring the differential activation signal for protein. Moreover, the authors in [142] calculated the channel capacity of the macroscale MC environment. Correspondingly, an upper bound on the capacity for a discrete-time compound Poisson channel was derived by authors in [143]. However, authors in [144] proposed new upper and lower bounds on the capacity for a point to point MC system. Meanwhile, an information-theoretic framework for analyzing MC systems on the basis of statistical mechanics was proposed by the authors in [145]. The authors in [146] attained a tight lower bound on the iid capacity of the constrained iid binding channel by utilizing a discrete input distribution. Concurrently, the authors in [147] obtained and compared the mutual information expressions for a two signal (electrochemical and mechanosensitive signals) intercellular communication observed mainly in plants. Further, the authors also studied the effect of the refractory period for both signals on mutual information. Moreover, the random cell motion leading to improvement in the cell to cell communication was highlighted by the authors in [148]. The authors first carried out cell tracing experiments of the endothelial cells in order to

acquire the value of motility parameters. Based on these values, the achievable rate for cellular communication was obtained. The authors utilized the various information-theoretic concepts in [149] to provide the closed-form expressions for the information rate for the case of neurotransmission. Utilizing the Poisson statistics, the authors highlighted the dependence of cells diversity on the information rate of the system. The authors in [150] proposed ISI mitigating channel codes for diffusive MC environments. The authors proposed an information-theoretic approach for modelling the target drug delivery in [151], wherein the practical implications of the target drug delivery system on the mutual information was observed. An achievable information rate for a mobile MC via multiple molecular measurements was highlighted by the authors in [152]. Simultaneously, the authors in [153] proposed a fundamental framework for investigating the effects of various chemical reactions on the information-theoretic capacity of diffusive MC systems. Notably, the authors obtained the expressions for various information-theoretic concepts. Finally, the authors observed via comparison that the channel capacity in a chemically reactive environment is less than that in an environment where there is no chemical reaction. An information-theoretic capacity expression was calculated for K^{+1} signalling ions by the authors in [154]. A mathematical model for illustrating the process of photosynthesis was highlighted by the authors in [155]. Similarly, an information-theoretic capacity for the ligand-based channel was investigated by authors in [156]. Further, the authors derived the upper and lower bounds on the mutual information for the Markov inputs. Meanwhile, the mutual information of the Kolmogorov turbulent system was calculated by the authors in [157].

2.3 Molecular Timing Channel

MC in which the information is modulated in the time of release of the information molecules corresponds to the molecular timing channel. The concept of molecular timing channel is not new and is found in many biological processes. The authors in [158] were the first one to highlight the timing channel in MC wherein the authors utilized the timing-based approach for modelling the communication scenario happening in the synaptic cleft of the brain. Consequently, the communication process between two chemical synapses over a chemical channel was also analyzed. Using the channels model as described in [158] the authors in [41] studied the bacterial communication over a microfluidic chip. Meanwhile, a detailed discussion about the practical applications of the timing-based communication channels, especially in biology,

was studied by authors in [129]. They illustrated the use of various biological particles to quantify the timing channels, which helped the authors in calculating the outer bounds on the timing channels. Simultaneously, the analysis of a timing-based channel was done by authors in [159], where the authors studied the transmission of bits through queues. In [159], the channel output, especially the arrival time of the information molecules, are ordered for the consecutive channel usage. This signifies that the first arrival time corresponds to the first channel use, the second arrival time corresponds to the second and so on. Similar to [159], the authors in [160] calculated the capacity of the point-process channel while the authors in [161] proposed a robust decoding method for the timing channels by taking in to consideration the orderly arrival of the queues. However, for the MC channels with indistinguishable molecules, the orderly arrival of the information molecules cannot be preserved at the receiving nanomachine. The information molecules transmitted during the first channel use may arrive after the information molecules are released during the second channel use. This scenario corresponds to the case where the order in which the information molecules transmitted by the transmitter is not preserved at the receiver. Therefore, the authors in [162] analyzed the channel capacity for the molecular timing channels where the order of information molecules is not preserved at the receiver.

The capacity calculation of the molecular timing channels is challenging when the information molecules arrive out of order at the receiver. Authors in [129], and [128] provided the bounds on the capacity expressions by taking an assumption that the receiver eventually receives all the information molecules and the average arrival time of these information molecules is finite. The authors in their book [163] focused on the additive inverse Gaussian (AIGN) channel for modelling the molecular timing channels. The authors employed the positive drift phenomenon in order to characterize the motion of information molecules in the AIGN channel, and based on this, authors observed that the first time of arrival over a one-dimensional space follows the inverse Gaussian distribution. Simultaneously in [17], upper and lower bounds on the capacity expression of the AIGN channel were calculated. These bounds calculations were presented based on the assumption that the average particle arrival time is constrained. In addition, to [17], the authors in [104] calculated different set of bounds on the capacity expression of the AIGN channel by considering the same set of constraints as used in [17]. Further, the authors in [106] implemented a different constraint which limits the maximum particle arrival time to calculate the expression on the upper bound of the channel capacity. Meanwhile, the bounds derived in [104] and [17] were further tightened by the authors in [105]. Further, to accurately

evaluate the capacity per channel use in the AIGN channel, the authors in [105] also characterized the capacity-achieving input distributions. The authors in [164] studied time-slotted transmission over molecular timing (MT) channels without the presence of external drift.

The authors in [83] calculated the capacity bounds expressions in terms of the symbol interval (τ_x), Lévy noise parameter (c) and particle lifetime (τ_n). Using physical parameters such as c and symbol interval (τ_x) the authors in [83] and [165] characterized the capacity bounds expression for single as well as multi-particle diffusion-based molecular timing (DBMT) channels. Furthermore, the capacity bounds on the DBMT channels using exponential degradation modelling was calculated in [80] and [82]. The authors in [80] and [82] introduced the concept of truncated Lévy distribution in order to model the random propagation delay. Moreover, the capacity of a discrete molecular diffusive channel was calculated in [166]. Additionally, M-array communication scheme for the macro-scale MT channels was analyzed as well as optimized in [167]. Moreover, the authors in [167] highlighted that macro-scale MT channels are ultra-reliable modes of MC. The authors in [7] studied transmission over DBMT channels without flow while assuming that the consecutive channel uses are independent and identically distributed (i.i.d). The authors also derived the ML detection rule, which according to the authors, requires high computational complexity and thus are not feasible for the nanoscale communication systems. Further, they proposed a new detector based on the first arrival (FA) time of the information molecules and analyzed the error performance of the system using this new detector. All of the above literature considered the synchronization process to model MT channel in MC scenario. However, the authors in [168] analyzed the DBMT channels in the asynchronous scenario wherein the receiver estimates the propagation time of the information molecules by taking into consideration the second-order moment of the arrival time of the molecules. Specifically, the authors proposed a symbol detection algorithm using the variance of the arrival times of information molecules that reached the receiver. Finally, the error probability of the proposed algorithm was derived. The effect of increasing the concentration of the released molecules on the error probability for different detection algorithms in the DBMT channels was studied by the authors in [169]. Compared to the analysis of the MT channels from the binary modulation perspective done by the authors in [168] and [169], the authors in [170] showed that M-array timing-based modulation scheme, especially for $M > 2$, outperforms the M-array concentration based modulation scheme. Concurrently, in [171] the authors proposed two new asynchronous modulation techniques for the DBMT channels. The first technique modulates information on

the time slot between two successive releases of information molecules, while the second technique uses distinguishable molecules. Based on these techniques, the authors then undertook the bit error rate (BER) analysis to evaluate the performance of the proposed system. Finally, the authors observed that the system with asynchronous modulation technique exhibits the highest BER compared to the BER analysis in the synchronous case. So by optimizing the timing of the receiver's observation an improvement in the error performance of the system was observed, and this improvement was significantly highlighted by the authors in [172]. Simultaneously, the authors in [172] proposed an improved sampling time for the amplitude detection, which in turn enhances the error performance of the system. Using the same constraints, the authors in [173] optimized the detection process timing in flow-based MC environments. The authors observed that by optimizing both sampling time and the number of observations at the receiver, the error performance of the system increases significantly.

The clock free asynchronous receiver design (CFARD) detector for DBMT channels was proposed by the author in [105]. Further, the proposed detector performance was compared with the existing detectors such as synchronous linear average filter (LAF), maximum synchronous likelihood (ML) detector and first arrival (FA) detectors. It was observed that the CFARD detector considerably lowers the structural complexity for information demodulation and helps in better employment of the system in environments with limitations of energy and size. Subsequently, the diversity in one-shot communication over MT channels was studied by authors in [174]. The authors characterized the asymptotic exponential decrease rate of the error probability as a function of the number of released information particles. Further, the authors expressed the asymptotic exponential decrease rate in terms of the diversity gain of the system since it is a function of transmitted information particles and the detection methods employed by the receiver. Finally, the authors observed that the FA detector is equivalent to the ML detector and can significantly outperforms the LAF detector. At the same time, the impact of time-synchronization in MT channels by analyzing three different modulation techniques was studied by authors in [175]. In the first scenario, the transmitter-receiver synchronization was proposed, whereas in the second and the third scenario asynchronous mechanism was employed for indistinguishable and distinguishable particles respectively. Due to the infinite variance of the stable distributions, the authors used the geometric power of a large class of stable distributions to quantify the strength of the noise. Therefore, by utilizing the geometric power of a large class of stable distributions, the authors further derived the geometric signal to noise ratio

(G-SNR) for each modulation scheme. In addition to G-SNR based calculation, the authors also calculated the optimal detection rules for each modulation technique. Finally, the authors observed that the BER is constant for a given G-SNR and the performance gain obtained for the synchronous case is significant. Further, for the asynchronous case the authors observed that instead of utilizing one type of information molecules if two distinguishable type of information particles per bit are employed, in the system, then the BER of the asynchronous technique approaches to that of the synchronous one. On the contrary, a clock along with the synchronization error into the MT channel scenario was introduced by the authors in [176]. The clock synchronization error in terms of variance constrained capacity, i.e., the capacity when the distribution of the delay (corresponding to messages) has both mean and variance constraints, was obtained. Further, to quantify the new clock-based system, the authors derived upper and lower bounds on the variance constrained capacity. The variance constrained capacity acts as a link between the mean delay and the peak delay constrained capacity. Finally, the authors analyzed that in order to achieve the variance constrained capacity with perfect synchronization, the drift velocity of the clock links does not need to be significantly larger than the drift velocity of the information link. The problem of zero-error communication through timing channels that can be interpreted as discrete-time queues with bounded waiting times was analyzed by the authors in [177]. In particular, capacity-achieving codes were explicitly constructed, and a linear time decoding algorithm for these codes was devised. An upper bound on the capacity of the DBMT channel with diversity was calculated by authors in [178]. Moreover, a fundamental framework for molecular communication channels, specifically in terms of the timing and payload, was studied by authors in [179].

To compute the performance of the DBMT channels based on optimal detectors, the authors in [180] derived a maximum-likelihood (ML) detector and then subsequently proposed a new low-complexity FA detectors. It was observed that for a small number of released particles, the performance of the FA detector is close to that of the ML detector. The authors undertook a receiver design for the MT channels in timing-based MC in [181]. First, the authors analyzed the timing based MC systems in the fluidic environment. Subsequently, they employed three detection approaches, namely the MAP detection, the average detection and the order statistic detection for designing the receiver. The near-optimal decision thresholds for average and order statistic detection were calculated when enough molecules were applied. Finally, the numerical results displayed that the order statistics detection is more robust to the change of fluid

coefficient out of all the three detection approaches.

2.4 Secrecy In Molecular Communication

The transmission of information securely from the transmitter to the receiver has always been a vital characteristic aspect in a communication systems scenario [182], [183], [184]. Thus the concept of secure transmission becomes imperative to be used in this relatively new field of communication since there is a propagation of privacy-sensitive information from the transmitter to the receiver [84]. Additionally, the elemental study of secure 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. The concept of secure communication in molecular communication was first highlighted in [182], wherein the challenges of physical layer security at the nanoscale level were presented. The authors observed that the existing security and cryptographic solutions might not be applicable for the MC scenario. To overcome this problem and maintain the information, architectural and structural integrity of the biological entity, bio-chemical cryptography was implemented. The authors also proposed that a new form of high-speed and energy-preserving security mechanisms can be developed using biochemical cryptography, which could protect the nanomachine from malicious attacks. Such bio-chemical cryptography derived its basis from the human immune system. A comprehensive overview of the MC systems from the security and privacy perspective was analyzed by the authors in [185]. The authors stated that for obtaining secrecy in MC systems, researchers from the multi-disciplinary backgrounds are needed. The authors also highlighted the issues and challenges related to security in MC systems. Simultaneously, a bio-chemical cryptography method to provide security and privacy was also considered.

The closed-form expression for the secrecy capacity was calculated in [183], wherein the secrecy capacity was dependent on the thermodynamic transmitter power, distance of eavesdropper, bandwidth of information signal and the radius of the receiver. The author in [183] used the capacity expression of [67] to obtain the secrecy in the MC scenario. Further, the authors observed that how for a given range of operations, the detection mechanism helps in achieving security from the transmit power perspective. Likewise, the concept of programmed biological entities modelling along with the cooperative motility and chemical sensing for the cellular entity was examined in [186]. Here, the authors introduced two attack scenarios, namely the

Blackhole scenario and Sentry attack scenario. In the Blackhole attack scenario, the malicious bio-nano things present in the environment emits attractant chemicals that draw the legitimate bio-nano things towards the malicious bio-nano things and prevent them from searching the target nodes. In contrast, in the Sentry attack scenario, the malicious bio-nano thing emits repellents to disperse the legitimate bio-nano thing from reaching its target. The authors also proposed some countermeasure strategies to combat the menace of the malicious node in MC.

Meanwhile, to achieve secure communication, an Energy-Saving algorithm was implemented by authors in [84], wherein secrecy was obtained by the Diffie-Hellman method. In particular, the communicating nanomachines exchange a secret key through molecular signalling, and this secret key is also used to achieve ciphering. Particularly, XOR ciphering to encrypt and decrypt the data using the generated secret key makes the system simple and effective in terms of energy consumption. A distance-based molecular cipher key was proposed by the authors in [187] so as to attain a viable and low-complexity physical layer security (PLS) algorithm for secure molecular communications. Moreover, the authors also observed that the achievable eavesdropper key disagreement rate (KDR) was 5 to 7 times higher than the intended transmission channel rate, demonstrating that an eavesdropper cannot decipher the transmitted messages. Subsequently, in [188] the authors demonstrated the potential of accurate passive eavesdropper detection and localization in molecular communications. For this, the authors used the attributes of the random-walk channel in order to detect and estimate the position of the eavesdropper accurately. Meanwhile, the authors in [189] highlighted various security issues in MC. The authors first tried to obtain the solution to the security issues in MC from the secrecy analysis perspective used in the traditional wireless networks. However, due to the nature of information propagation being molecular, direct one to one analogy was not possible. Further, the authors also studied various security issues in nanonetworks based on EM wave-spectrum and highlighted some protocols to address the security problem in these nanonetworks. In addition to this, the authors also analyzed the secrecy in molecular-based nanonetworks, where they also mentioned the Blackhole attack scenario and Sentry attack scenario. Here, the authors mentioned that the secure transmission of information in vesicle-based molecular transport environment can be achieved by employing various vesicles acting as a secure key. Finally, the authors also illustrated the security scenario in hybrid based nanoscale communication.

The authors proposed a new, lightweight body area network authentication (BANA) scheme in [190]. The so-called BANA protocol addresses the security needs of the micro-macro link

of a body area network; as the BANA protocol is independent of the prior trust among nodes and can be efficiently realized on commercial off the shelf low-end sensors. The BANA protocol was achieved by exploiting a unique characteristic, i.e., the distinct received signal strength (RSS), of the physical layer of the body area network. This distinct RSS variation enables the BANA protocol to adopt the clustering analysis, enabling the signal to differentiate between the legitimate node and an eavesdropper. Further, the authors used a multi-hop approach to enhance the system's robustness. Meanwhile, the authors in [191] presented physical layer authentication of nano-networks at THz frequencies for biomedical applications. Specifically, the authors considered an in vivo body-centric nano-communication and based on the system model, a distance-dependent path-loss based authentication was performed. From the experimental data collected from THz time-domain spectroscopy setup, the authors concluded that path-loss could be employed as a fingerprint for the devices, which would then be used to achieve secure communication in THz base nano-networks. Simultaneously, the author in [192] discussed DNA based approach to provide information security in molecular biology. Additionally, the use of DNA molecules for providing biochemical cryptography is not new and has already been reported in the literature. Specifically, the authors in [193] used the microdot for developing a DNA-based, doubly steganographic technique for achieving secrecy. Similarly, the authors in [194] employed various biotechnological methods to attain cryptography. In the first approach, the authors proposed how DNA binary strands can be used for DNA steganography. It was observed that the DNA steganography method based on DNA binary strands is secure under the assumption that an interceptor has the same technological capabilities as transmitter and receiver. Finally, the authors proposed that DNA steganography can be applied to provide security to the practical systems, primarily where labelling of organic and inorganic materials can be accomplished with the help of DNA barcodes. Likewise, the authors in [195], and [196] extensively worked on DNA inspired cryptography in order to provide security in biological systems. A machine learning (ML) based technique was employed by the authors in [197] so as to provide security in the internet of bio-nano things (IoBNT). The authors employed various decision tree classifiers to represent the operational features of three different bio-cyber interfaces: bio-luminescent, redox modality, and bio-FETs. Consequently, using the time complexity analysis, the authors observed that the proposed security solution exhibits low latency and high scalability. Lastly, the authors explored the effect of an unintended nanomachine (UN) on the performance of a 3-D diffusive point to point MC in [198]. The authors employed two

different scenarios to analyze the effect of UN in diffusive MC. In the first scenario, the UN was considered an unintended transmitter nanomachine (UTN), and therefore average error probability and maximum achievable rate were calculated. Subsequently, in the second scenario, the UN was considered an unintended receiver nanomachine (URN), and the system performance in terms of the information leakage and maximum achievable secrecy rate was undertaken. Finally, in both cases, an optimal detector was implemented to attain optimal secrecy performance.

From the literature, it emerges that the issues related to secrecy performance in DBMT channels have not been appropriately addressed. Therefore, an attempt has been made to address the secrecy performance of the DBMT channels from average eavesdropper capacity, fractional equivocation, generalized secrecy outage probability, amount of confusion level and secrecy loss perspective.

Chapter 3

Secrecy Of Single-Particle DBMT channels

3.1 Introduction

MC is nowadays considered a viable option in environments where conventional communication systems fail to deliver favourable results. Since MC is usually employed in the human healthcare environment, where there is a plethora of confidential information, it becomes critical to analyze the secrecy perspective in the begining rather than incorporating security to these MC systems at the later stages. Incorporating security at the later stage can cause design complications, leading to a loss of interest in this promising field. Therefore, in this chapter, the secrecy performance of a single-particle DBMT channel is studied. We employ PLS wherein various secrecy performance metrics are used to analyze the system's secrecy. Since PLS is independent of the eavesdropper's computational abilities, it can be considered a handy tool to combat the menace of an eavesdropper. Moreover, the information-theoretic secrecy deals in calculating exactly how much amount of confidential information is accessible to an eavesdropper. This type of secrecy is referred to as the classical secrecy regime. In the classical secrecy regime, secrecy is usually undertaken when the eavesdropper observes the communication happening between the transmitter and the legitimate node. Usually, the amount of information stolen by the eavesdropper is represented by the eavesdropper capacity from an information-theoretic sense. Therefore, the secrecy capacity of any communication system, including the diffusive MC systems, corresponds to the maximum of the difference between Bob's capacity and eavesdropper capacity. So the secrecy capacity analysis, which primarily comprises of the upper bound of the average eavesdropper capacity when the distance of eavesdropper is assumed to be uniform and Gaussian distributed, is undertaken. Subsequently, the

secrecy performance from the fractional equivocation perspective is also proposed in this chapter. Fractional equivocation is a metric used to quantify the partial secrecy regime and signifies the confusion level of Eve. Therefore, secrecy evaluation based on equivocation corresponds to Eve's message decodability. Since, no one-to-one relationship exists between equivocation and the error probability, it is advantageous to lower bound the decoding error probability in terms of equivocation. Therefore, in this chapter, the secrecy performance from the fractional equivocation perspective is proposed.

3.2 System Model

The system model for the Diffusion-based molecular communication embodies a transmitting 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 3.1. The transmitting point source enclosed within the physical system is proficiently transmitting the molecules of identical nature.

Similar to [80] 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_n. Mathematically, the time of arrival at the receiver is expressed as:

$$T_a = T_t + T_n. \tag{3.1}$$

The propagation delay (T_n) for the drift free scenario can be modeled as α-stable Lévy distributed random variable (RV) (Lévy(μ, c)) [81]. Mathematically, Lévy distributed RV, R can be represented as:

$$f_R(r;\mu,c) = \sqrt{\frac{c}{2\pi(r-\mu)^3}}\exp\left(-\frac{c}{2(r-\mu)}\right), \tag{3.2}$$

where μ is location parameter and c is scale parameter. The propagation delay time (T_n) is basically the additive noise term which can be written as $T_n \sim$Lévy$(0, d^2/(2D))$ and mathematically

expressed as [80]:

$$f_{T_n}(t_n) = \frac{d}{\sqrt{4\pi D t_n^3}} \exp\left(-\frac{d^2}{4D(t_n)}\right). \tag{3.3}$$

The rate at which these molecules die-out is determined by the degradation parameter denoted as α, mathematically which is modeled as [80]:

$$h(\tau) = \alpha \mathrm{e}^{-\alpha\tau}, \qquad \tau > 0, \tag{3.4}$$

where α is the *degradation parameter*, τ is the *lifetime* of the molecules and $h(\tau)$ 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 RV (t_d) [80], which mathematically is represented as:

$$f_{t_d} = \begin{cases} 0, & \text{for} \quad t_d \leq 0, \\ \sqrt{\frac{d^2}{4\pi D t_d^3}}\, \mathrm{e}^{-\frac{d^2}{4Dt_d}}\, \mathrm{e}^{-\alpha(t_d)}, & \text{for} \quad t_d > 0, \end{cases} \tag{3.5}$$

where c 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,i.e., 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 η and the temperature (T) of the aqueous media.

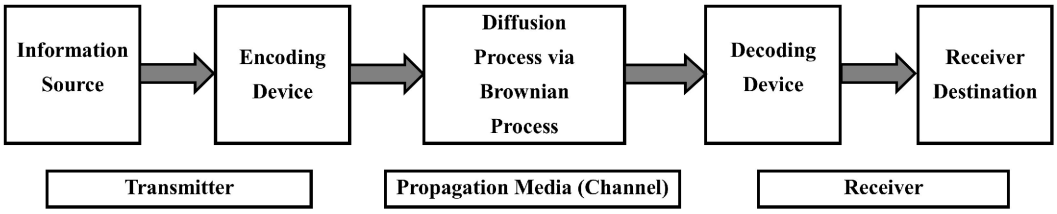

Figure 3.1: Block diagram of diffusion-based molecular communication [183].

- 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 generalized secrecy outage probability, average fractional equivocation and average information leakage rate are what that leads to the fundamental theory of any secure communication.

3.3 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:

$$C = \max_{f_X(x)} I(X:Y) = \max_{f_X(x)} H(X) - H(X/Y), \tag{3.6}$$

where $I(X:Y) = I(T_t;T_a)$ that is the mutual information maximization is based in terms of the transmit time (T_t) and the receiving or arrival time (T_a).

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 [80] whose mathematical portrayal is represented as:

$$\begin{aligned} C_{ub} \leq & \ln\left(\left(\tau_x + \frac{c}{p}\mathrm{e}^{-p}\right)e\right) + \frac{3}{2}\sqrt{\frac{p}{2\pi}}I_{1/2}(p)\ln\left(\frac{p}{c}\right) \\ & - \frac{\mathrm{e}^{-p}}{2}\left(1+2p-\ln\left(\frac{c}{2\pi}\right) - \frac{1}{\pi}(\mathrm{e}^{2p}Ei(-2p) - Ei(2p))\right), \end{aligned} \tag{3.7}$$

where

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

The average waiting time between the consecutive transmission is given as

$$\tau_s \gg \tau_x + \mathbf{E}(T_n), \tag{3.8}$$

and expectation obtained from [80] is represented as

$$\mathbf{E}(T_n) = \mathrm{e}^{-p}\left(\sqrt{\frac{c}{2\alpha}}\right). \tag{3.9}$$

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 the equation (3.7). According to Figure 3.2, 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_S). 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 [183]:

$$I(X;Z) = H(X) - H(X/Z), \tag{3.10}$$

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 3.2, we have assumed that Bob is present at a fixed distance with respect

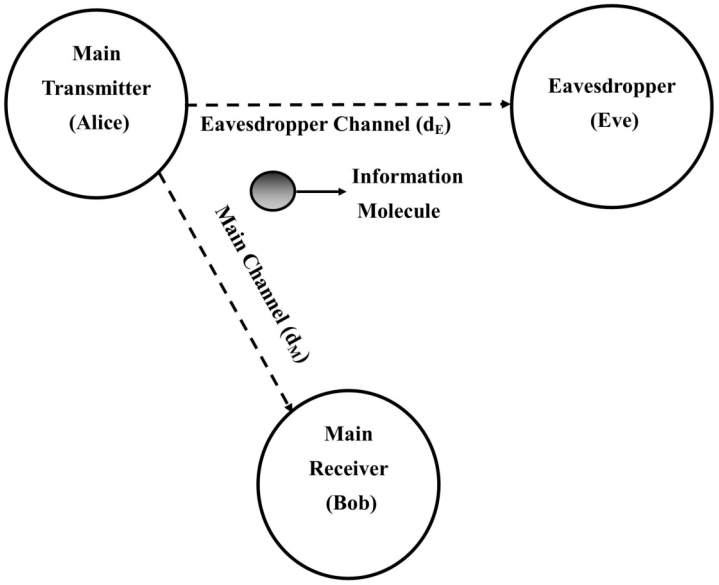

Figure 3.2: Scenario of eavesdropping in diffusion-based molecular communication.

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.

3.3.1 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 RV $\mathscr{U}(0,d_E)$ having a certain probability density function (p.d.f). Now, using the upper bound given by (3.7) the upper bound of average eavesdropper capacity can be calculated by,

$$C_E = \int_0^{d_E} f_d(d)\, C_{ub}\, dx. \tag{3.11}$$

On substituting (3.7) into (3.11) and using the p.d.f of uniform distribution we get:

$$\begin{aligned} C_E = \int_0^{d_E} \frac{1}{d_E} \Bigg[& \ln\left(\left(\tau_s + \frac{c}{p}\mathrm{e}^{-p}\right) e\right) + \frac{3}{2}\sqrt{\frac{p}{2\pi}} I_{1/2}(p) \ln\left(\frac{p}{c}\right) \\ & - \frac{\mathrm{e}^{-p}}{2}\left(1 + 2p - \ln\left(\frac{c}{2\pi}\right) - \frac{1}{\pi}(\mathrm{e}^{2p} Ei(-2p) - Ei(2p))\right)\Bigg]\, dx. \end{aligned} \tag{3.12}$$

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

$$f_p(p) = \begin{cases} \frac{1}{d_E}\left(\sqrt{\frac{D}{\alpha}}\right), & \text{for } 0 \leq p \leq d_E\left(\sqrt{\frac{\alpha}{D}}\right), \\ 0, & \text{otherwise.} \end{cases} \tag{3.13}$$

In order to obtain a closed-form solution of (3.12) we bifurcate the upper bound of average eavesdropper capacity equation into three integrals of I_{E_1}, I_{E_2} and I_{E_3}. These three integral values in mathematical relationship with eavesdropper capacity is represented as:

$$C_E = I_{E_1} + I_{E_2} + I_{E_3}, \tag{3.14}$$

where,

$$I_{E_1} = \int_0^{d_E} \frac{1}{d_E} \ln\left(\left(\tau_s + \frac{c}{p}\mathrm{e}^{-p}\right)e\right) dx. \tag{3.15}$$

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

$$I_{E_1} = d_E \ln(\tau_s) + d_E + \frac{{d_E}^2}{2} - \frac{{d_E}^2}{2}\sqrt{\frac{\alpha}{D}} + \sum_{n\geq 1} \frac{(-1)^{n+1}}{n^{n+2}} \left(\gamma(n+1, nd_E)\right), \tag{3.16}$$

where, $\gamma(n+1, nd_E)$ is the lower incomplete gamma function. From (3.16) it can observed that I_{E_1} is the average capacity component of Eve link which is a function of τ_s. On the similar grounds, the mathematical representation of the integral I_{E_2} is given as:

$$I_{E_2} = \left(\frac{3}{2\sqrt{2\pi}}\right)\left(\frac{D}{d_E\alpha}\right)\int_0^{p1} p^{1/2} I_{1/2}(p)\left(\ln(2\alpha) - \ln(p)\right) dp, \tag{3.17}$$

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

$$\begin{aligned} I_{E_2} = \left(\frac{3}{2\sqrt{2\pi}}\right)\left(\frac{D}{d_E\,\alpha}\right)\Big[&\sqrt{p_1}\, I_{-1/2}(p_1)\ln(2\alpha) - p_1^{3/2}\, I_{1/2}(p_1)\ln(p_1) + p_1^{3/2}\, I_{1/2}(p_1) \\ &+ \ln(p_1)\, p_1^{3/2}\, I_{3/2}(p_1) - \frac{(\mathrm{e}^{p_1}-1)}{\sqrt{2\pi}} - \frac{2}{\pi}\left(\log(p_1)\right) p_1^{3/2}\, K_{-3/2}(p_1) \\ &+ \sqrt{\frac{2}{\pi}}\left(1-\mathrm{e}^{-p_1}\right)\Big], \end{aligned} \tag{3.18}$$

where, $I_{-1/2}, I_{1/2}, I_{3/2}$ and $K_{-3/2}$ are the mathematical notation for modified Bessel's Functions respectively. From (3.18) it can be observed that I_{E_2} is a function of system parameters such as α and D. Moreover, I_{E_2} being average capacity component of Eve link is independent of τ_s. The mathematical expression for the third integral (I_{E_3}) as given in (3.14) is illustrated as:

$$I_{E_3} = \frac{-1}{d_E}\int_0^{d_E} \frac{\mathrm{e}^{-p}}{2}\left(1+2p-\ln\left(\frac{c}{2\pi}\right)-\frac{1}{\pi}(\mathrm{e}^{2p}Ei(-2p)-Ei(2p))\right)dx, \tag{3.19}$$

where, $p = d_E\sqrt{\frac{\alpha}{D}}$. In order to obtain the closed-form expression of the above integral we bifurcate this 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 (3.19) is obtained as under:

$$\begin{aligned} I_{E_3} =& \frac{-1}{d_E}\left[\frac{\sqrt{D}\,(1-\mathrm{e}^{-d_E\sqrt{\frac{\alpha}{D}}})}{2\sqrt{\alpha}} + d_E\mathrm{e}^{-d_E} + \mathrm{e}^{-d_E} - 1 + \left(\ln(d_E)\frac{\mathrm{e}^{-d_E\sqrt{\frac{\alpha}{D}}}}{\sqrt{\frac{\alpha}{D}}}\right) - Ei\left(-d_E\sqrt{\frac{\alpha}{D}}\right)\right. \\ &+ \left(\frac{\ln(4\pi D)}{2}\right)\left(\frac{1-\mathrm{e}^{-d_E\sqrt{\frac{\alpha}{D}}}}{\sqrt{\frac{\alpha}{D}}}\right) - \sqrt{\frac{D}{\alpha}}\left(\mathrm{e}^{(d_E\sqrt{\frac{\alpha}{D}})}Ei\left(-2d_E\sqrt{\frac{\alpha}{D}}\right) - Ei\left(-d_E\sqrt{\frac{\alpha}{D}}\right)\right) \\ &\left. - \sqrt{\frac{D}{\alpha}}\left(\mathrm{e}^{-(d_E\sqrt{\frac{\alpha}{D}})}Ei\left(2d_E\sqrt{\frac{\alpha}{D}}\right) - Ei\left(d_E\sqrt{\frac{\alpha}{D}}\right)\right)\right]. \end{aligned} \tag{3.20}$$

Substituting (3.16), (3.18) and (3.20) into (3.14) 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 (α), diffusion coefficient (D) and τ_s. 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_{E_1} component shows the dependence of 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).

3.3.2 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 μ_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:

$$C_E = \int_0^{d_E} f_x(x)\, C_{ub}\, dx. \tag{3.21}$$

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

$$f_p(p) = \frac{1}{\sqrt{2\pi\sigma_p^2}}\, \mathrm{e}^{-\frac{(p-\mu_p)^2}{2\sigma_p^2}} \quad \text{for} \quad 0 \le p \le d\left(\sqrt{\alpha/D}\right), \tag{3.22}$$

where μ_p is the mean of this new RV having value $\mu_p = \sqrt{\frac{\alpha}{D}}\, \mu_x$ and σ_p^2 is the variance of the p RV with $\sigma_p^2 = \frac{\alpha}{D}\, \sigma_x^2$. Therefore, by substituting (3.7) into (3.21) we are able to obtain the eavesdropper capacity expression.

$$\begin{aligned} C_E = \int_0^{d_E} \left(\frac{1}{\sqrt{2\pi\sigma_x^2}}\, \mathrm{e}^{-\frac{(x-\mu_x)^2}{2\sigma_x^2}}\right) \Bigg[\ln\left(\left(\tau_s + \frac{c}{p}\mathrm{e}^{-p}\right)\mathrm{e}\right) + \frac{3}{2}\sqrt{\frac{p}{2\pi}} I_{1/2}(p) \ln\left(\frac{p}{c}\right) \\ - \frac{\mathrm{e}^{-p}}{2}\left(1 + 2p - \ln\left(\frac{c}{2\pi}\right) - \frac{1}{\pi}(\mathrm{e}^{2p} Ei(-2p) - Ei(2p))\right)\Bigg]\, dx. \end{aligned} \tag{3.23}$$

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 (3.23) is obtained as:

$$C_E = I_{E_1} + I_{E_2} + I_{E_3}, \tag{3.24}$$

where

$$I_{E_1} = \int_0^{d_E} \left(\frac{1}{\sqrt{2\pi\sigma_x^2}}\, \mathrm{e}^{-\frac{(x-\mu_x)^2}{2\sigma_x^2}}\right) \ln\left(\left(\tau_s + \frac{c}{p}\mathrm{e}^{-p}\right)\mathrm{e}\right) dx. \tag{3.25}$$

The closed-form expression of (3.25) is obtained in (3.26), which is given as

$$\begin{aligned} I_{E_1} =& \frac{1}{2\sqrt{2\sigma_p^2}}\left(F_1\ln(\tau_s)+F_2+F_3+F_4+F_5+\frac{\sqrt{2\sigma_p^2}}{2\alpha\tau_s}\left[F_6+F_7+F_8\frac{\mu_p}{\sqrt{2\sigma_p^2}}\right]\right. \\ & \left.-\frac{\sqrt{2\sigma_p^2}}{2\alpha\tau_s}\left[F_9+F_{10}+F_{11}\frac{\mu_p}{\sqrt{2\sigma_p^2}}\right]\right), \end{aligned} \tag{3.26}$$

where

$$F_1 = \frac{1}{\sqrt{a_{11}}}\mathrm{e}^{\left(\frac{b_{11}^2-a_{11}c_{11}}{a_{11}}\right)}\mathrm{erf}\left(p_1\sqrt{a_{11}}+\frac{b_{11}}{\sqrt{a_{11}}}\right)-\frac{1}{\sqrt{a_{11}}}\mathrm{e}^{\left(\frac{b_{11}^2-a_{11}c_{11}}{a_{11}}\right)}\mathrm{erf}\left(\frac{b_{11}}{\sqrt{a_{11}}}\right), \tag{3.27}$$

$$F_2 = \frac{1}{\sqrt{a_{12}}}\mathrm{e}^{\left(\frac{b_{12}^2-a_{12}c_{12}}{a_{12}}\right)}\mathrm{erf}\left(p_1\sqrt{a_{12}}+\frac{b_{12}}{\sqrt{a_{12}}}\right)-\frac{1}{\sqrt{a_{12}}}\mathrm{e}^{\left(\frac{b_{12}^2-a_{12}c_{12}}{a_{12}}\right)}\mathrm{erf}\left(\frac{b_{12}}{\sqrt{a_{12}}}\right), \tag{3.28}$$

$$F_3 = \sqrt{\frac{2}{a_{13}}}\left(\ln\left(1+\frac{p_1\mathrm{e}^{-p_1}}{2\alpha\tau_s}\right)\right)\mathrm{e}^{\left(\frac{b_{13}^2-a_{13}c_{13}}{a_{13}}\right)}\mathrm{erf}\left(p_1\sqrt{a_{13}}+\frac{b_{13}}{\sqrt{a_{13}}}\right), \tag{3.29}$$

$$F_4 = \frac{\mathrm{e}^{-p_1}}{2\alpha\tau_s}\mathrm{erf}\left(\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}\right), \tag{3.30}$$

$$F_5 = \frac{\mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}}{2\alpha\tau_s}\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}}-\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}\right), \tag{3.31}$$

$$F_6 = -\frac{\mathrm{e}^{-p_1}}{2\alpha\tau_s}\mathrm{erf}\left(\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}\right)\left(\frac{p_1-\mu_p+1}{\sqrt{2\sigma_p^2}}\right), \tag{3.32}$$

$$\begin{aligned} F_7 =& \mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}\left(\frac{1}{\sqrt{2\sigma_p^2}}-\sqrt{\frac{\sigma_p^2}{2}}\right)\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}}-\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}\right) \\ & -\mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}\frac{1}{\sqrt{\pi}}\mathrm{e}^{-\left(\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}+\sqrt{\frac{\sigma_p^2}{2}}\right)^2}, \end{aligned} \tag{3.33}$$

$$F_8 = -\mathrm{e}^{-p_1}\mathrm{erf}\left(\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}\right)+\mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}}-\frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}\right), \tag{3.34}$$

$$F_9 = -\frac{1}{2\alpha\tau_s}\mathrm{erf}\left(\frac{-\mu_p}{\sqrt{2\sigma_p^2}}\right)\left(\frac{-\mu_p+1}{\sqrt{2\sigma_p^2}}\right), \tag{3.35}$$

$$\begin{aligned} F_{10} =& \mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}\left(\frac{1}{\sqrt{2\sigma_p^2}}-\sqrt{\frac{\sigma_p^2}{2}}\right)\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}}-\frac{-\mu_p}{\sqrt{2\sigma_p^2}}\right) \\ & -\mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}\frac{1}{\sqrt{\pi}}\mathrm{e}^{-\left(\frac{-\mu_p}{\sqrt{2\sigma_p^2}}+\sqrt{\frac{\sigma_p^2}{2}}\right)^2}, \end{aligned} \tag{3.36}$$

$$F_{11} = -\mathrm{erf}\left(\frac{-\mu_p}{\sqrt{2\sigma_p^2}}\right)+\mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}}-\frac{-\mu_p}{\sqrt{2\sigma_p^2}}\right). \tag{3.37}$$

Here $p_1 = \left(d_E\sqrt{\frac{\alpha}{D}}\right)$, $a_{11} = a_{12} = a_{13} = \left(\frac{1}{2\sigma_p^2}\right)$, $b_{11} = b_{12} = b_{13} = \left(\frac{-\mu_p}{2\sigma_p^2}\right)$, $c_{11} = c_{12} = c_{13} = \left(\frac{\mu_p^2}{2\sigma_p^2}\right)$. From (3.26) it can be noted that the average Eve capacity component (I_{E_1}) is a function of τ_s, α, mean of eavesdropper distance (μ_x) and variance (σ_E^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 (3.24) is given as:

$$I_{E_2} = \frac{3}{2}\int_0^{p_1}\sqrt{\frac{p}{2\pi}}I_{1/2}(p)\ln\left(\frac{2\alpha}{p}\right)\left(\frac{1}{\sqrt{2\pi\sigma_p^2}}\mathrm{e}^{-\frac{(p-\mu_p)^2}{2\sigma_p^2}}\right)dp. \tag{3.38}$$

In (3.38) 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:

$$I_{1/2}(p) = \sqrt{\frac{2}{\pi}}\frac{\mathrm{Sinh}(p)}{\sqrt{p}}. \tag{3.39}$$

Now by substituting (3.39) in (3.38) 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:

$$I_{E_2} = \frac{3(\ln(2\alpha))}{4\pi\sqrt{\sigma_p^2}}\Bigg[\left\{\sigma_p\,\mathrm{Sinh}(t_1)\mathrm{erf}(t_1) - \sigma_p\,\mathrm{Sinh}(t_0)\mathrm{erf}(t_0)\right\} - \frac{(\sigma_p)\mathrm{e}^{\mu_p}}{2\sqrt{2\sigma_p^2}}\Bigg\{\mathrm{e}^{t_1\sqrt{2\sigma_p^2}}\mathrm{erf}(t_1) + \mathrm{e}^{\left(\frac{\sigma_p^2}{2}\right)}\mathrm{erf}\left(\sqrt{\frac{\sigma_p^2}{2}} - t_1\right) - \mathrm{e}^{t_0\sqrt{2\sigma_p^2}}\mathrm{erf}(t_0) - \mathrm{e}^{\left(\frac{\sigma_p^2}{2}\right)}\mathrm{erf}\left(\sqrt{\frac{\sigma_p^2}{2}} - t_0\right)\Bigg\} - \frac{(\sigma_p)\mathrm{e}^{-\mu_p}}{2\sqrt{2\sigma_p^2}}\Bigg\{\mathrm{e}^{-t_1\sqrt{2\sigma_p^2}}\mathrm{erf}(t_1) + \mathrm{e}^{\left(\frac{\sigma_p^2}{2}\right)}\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}} - t_1\right) - \mathrm{e}^{-t_0\sqrt{2\sigma_p^2}}\mathrm{erf}(t_0) - \mathrm{e}^{\left(\frac{\sigma_p^2}{2}\right)}\mathrm{erf}\left(-\sqrt{\frac{\sigma_p^2}{2}} - t_0\right)\Bigg\}\Bigg], \tag{3.40}$$

where $t_1 = \frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}$ and $t_0 = \frac{-\mu_p}{\sqrt{2\sigma_p^2}}$ respectively. From (3.40) it can be observed that the average Eve capacity component (I_{E_1}) is a function of α, scaled version of Lévy noise parameter (p), μ_x and σ_E^2. 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:

$$I_{E_3} = \frac{1}{\sqrt{2\pi\sigma_p^2}}\int_0^{d_E}\frac{\mathrm{e}^{-p}}{2}\left(1+2p-\ln\left(\frac{c}{2\pi}\right)-\frac{1}{\pi}(\mathrm{e}^{2p}Ei(-2p)-Ei(2p))\right)\mathrm{e}^{-\frac{(p-\mu_p)^2}{2\sigma_p^2}}\,dx, \tag{3.41}$$

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

$$I_{E_3} = \Bigg[\frac{\mathrm{e}^{\left(\frac{\sigma_p^2}{2}-\mu_p\right)}}{4}\left[\mathrm{erf}\left(t_1+\sqrt{\frac{\sigma_p^2}{2}}\right)-\mathrm{erf}\left(t_0+\sqrt{\frac{\sigma_p^2}{2}}\right)\right] + \frac{1}{\sqrt{2\pi\sigma_p^2}}\Bigg\{\frac{b_{31}\sqrt{\pi}\mathrm{e}^{\left(c_{31}+\frac{b_{31}^2}{4a_{31}}\right)}}{4(a_{31})^{3/2}} - \sigma_p^2\mathrm{e}^{\left(\frac{-p_1^2}{2\sigma_p^2}+\frac{\mu_p^2}{2\sigma_p^2}-p_1\left(\frac{\mu_p}{\sigma_p^2-1}\right)\right)} + \sigma_p^2\mathrm{e}^{\left(-\frac{\mu_p^2}{2\sigma_p^2}\right)}\Bigg\} + \frac{\ln(4\pi\alpha)\,\mathrm{e}^{\left(-\mu_p+\frac{\sigma_p^2}{2}\right)}}{4}\Bigg\{\mathrm{erf}\left(t_1+\sqrt{\frac{\sigma_p^2}{2}}\right) - \mathrm{erf}\left(t_0+\sqrt{\frac{\sigma_p^2}{2}}\right)\Bigg\}\Bigg], \tag{3.42}$$

where $t_1 = \frac{p_1-\mu_p}{\sqrt{2\sigma_p^2}}$ and $t_0 = \frac{-\mu_p}{\sqrt{2\sigma_p^2}}$ respectively. Thus after obtaining the closed-form expression for the integrals I_{E_1}, I_{E_2} and I_{E_3}, we now substitute (3.26), (3.40) and (3.42) in (3.24) so as to

obtain the upper bound of eavesdropper capacity for Gaussian distributed RV. 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 (α), diffusion coefficient (D), mean of eavesdropper distance (μ_x), variance (σ_E^2), etc. Also, I_{E_1} component of (3.24) 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 prefect 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 generalized 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.

3.4 Secrecy Performance Analysis

Consider the basic wiretap channel, as shown in Figure 3.2. 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, i.e., $\delta \to 1$. Meanwhile, the conventional secrecy analysis fails when Eve's decoding error probability (δ) ranges from 0 to 1, i.e., $0 < \delta \leq 1$. Thus instead of conventional secrecy outage probability, we now use three secrecy metrics: generalized secrecy outage probability (P_{out}), average fractional equivocation $(\bar{\Delta})$ and average information leakage (R_L).

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

(Δ) as defined in [199], [200] mathematically is represented as:

$$\Delta = \frac{H(X|Z)}{H(X)}. \tag{3.43}$$

For the wireless scenario the fractional equivocation is given in [199, eq.7] where C_b, C_e were main channel and eavesdropper capacities and R was the secrecy rate. In [199] 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 [199] was obtained as:

$$\Delta = \begin{cases} 1, & \text{for} \quad C_E \leq C_M - R_s \\ \frac{C_M - C_E}{R_s}, & \text{for} \quad C_M - R_s < C_E < C_M \\ 0, & \text{for} \quad C_M \leq C_E, \end{cases} \tag{3.44}$$

where, Δ =fractional equivocation. Notice that these three conditions for Δ represent different levels of confusion at Eve. First, when $C_E \leq C_M - R_s$, 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 $\Delta = \frac{(C_M - C_E)}{R_s}$ represents a partial secrecy regime, in which only a fraction of the communication is secure. Unlike the conventional equivocation as explained in [201, eq.(2)], the fractional equivocation as given by (3.43) 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,

$$C_E \approx 1 + \ln(d_E) - \ln\left(\sqrt{4D\alpha}\right). \tag{3.45}$$

The fractional equivocation as given by (3.44) can be modified in terms of eavesdropper distance as:

$$\Delta = \begin{cases} 1, & \text{for} \quad d_E \leq \mathrm{e}^{R_b - R_s - A} \\ \frac{R_b - \ln(d_E) - A}{R_s}, & \text{for} \quad \mathrm{e}^{R_b - R_s - A} < d_E < \mathrm{e}^{R_b - A} \\ 0, & \text{for} \quad \mathrm{e}^{R_b - A} \leq d_E, \end{cases} \tag{3.46}$$

where $A = 1 - \ln(\sqrt{4D\alpha})$ and $R_b \leq C_M$. The following subsections show the detailed analysis of three metrics (generalized 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.

3.4.1 Generalized Secrecy Outage Probability

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

$$P_{out} = \mathbb{P}(\Delta < \phi), \tag{3.47}$$

where $\mathbb{P}(.)$ is the probability function of an event and ϕ 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 $C_E \leq C_M - R_s$, which corresponds to case when $\phi = 1$. Since the fractional equivocation denotes the decoding error probability of the eavesdropper, thus generalized secrecy outage probability is applicable for all practical scenarios. Moreover, the conventional secrecy outage probability is a special case of generalized secrecy outage probability metric. Using (3.46) the expression for generalized secrecy outage probability can be obtained as:

$$\begin{aligned} P_{out} =& \mathbb{P}(d_E \geq \mathrm{e}^{R_b - A}) + \mathbb{P}(\mathrm{e}^{R_b - R_s - A} < d_E < \mathrm{e}^{R_b - A}) \\ & \times \mathbb{P}\left(\frac{R_b - \ln(d_E) - A}{R_s} < \phi \middle| \mathrm{e}^{R_b - R_s - A} < d_E < \mathrm{e}^{R_b - A} \right). \end{aligned} \tag{3.48}$$

3.4.2 Average Fractional Equivocation

The average fractional equivocation is defined as expectation of fractional equivocation. By taking expectation of (3.46) we can obtain the value of average fractional equivocation. Mathematically the average fractional expectation is given as

$$\bar{\Delta} = \mathbb{E}(\Delta), \tag{3.49}$$

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

3.4.3 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:

$$R_L = \mathbb{E}\{(1-\Delta)R_s\} = (1-\bar{\Delta})R_s, \tag{3.50}$$

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.

3.5 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 (3.48) the expression for generalized secrecy outage probability when eavesdropper distance is uniform distributed is obtained as:

$$P_{out} = \int_{\beta}^{d_E} \frac{1}{d_E}\, dx + \int_{\beta_1}^{\beta} \frac{1}{d_E}\, dx, \tag{3.51}$$

where $\beta_1 = \mathrm{e}^{R_b - R_s\phi - A}$ and $\beta = \mathrm{e}^{R_b - A}$. Finally, by substituting β and β_1 in (3.51) we obtain generalized secrecy outage probability as

$$P_{out} = 1 - \frac{\mathrm{e}^{R_b - R_s\phi - A}}{d_E}, \tag{3.52}$$

where $A = 1 - \ln(\sqrt{4D\alpha})$ and $0 < \phi \leq 1$. In general, for any value of ϕ, $0 < \phi \leq 1$, the Taylor series expansion of (3.52), which gives generalized secrecy outage probability for $R_b > R_s$, can be represented as:

$$P_{out} = 1 - \frac{1}{\sqrt{12\sigma_x^2}} - \frac{(R_b - R_s\phi - A)}{\sqrt{12\sigma_x^2}} - O(R_b - R_s\phi - A) \tag{3.53}$$

where, $O(R_b - R_s\phi - A)$ represents the other higher order terms. Now comparing (3.53) with

$$P_{out}^{\infty} = \left(G_c\sigma_x^2\right)^{-G_d} + O(\sigma_x^2)^{-G_d}, \tag{3.54}$$

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

$$G_d = \frac{1}{2}, \tag{3.55}$$

and

$$G_c = \frac{\sqrt{12}}{A + R_s\phi - R_b}. \tag{3.56}$$

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 α, D, d_M, d_E etc.
- Secrecy Gain increases with the increase in the main channel rate R_b.
- For a higher value of α 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 ϕ. G_c is inversely proportional to ϕ, i.e, for ϕ ranging from 0 to 1 the secrecy gain G_c degrades.

For $\phi = 1$ the equation (3.52) reduces to special case of classical secrecy outage probability which is given as:

$$P_{out} = 1 - \frac{\mathrm{e}^{R_b - R_s - A}}{d_E}. \tag{3.57}$$

Using Taylor series expansion in (3.57), and also substituting $d_E = \sqrt{12\sigma_x^2}$, the outage probability for $R_b > R_s$ can be represented as

$$P_{out} = 1 - \frac{1}{\sqrt{12\sigma_x^2}} - \frac{(R_b - R_s - A)}{\sqrt{12\sigma_x^2}} - O(R_b - R_s - A) \tag{3.58}$$

where, $O(R_b - R_s - A)$ represents the other higher order terms. Now by comparing (3.58) with (3.54) we obtain the values of diversity gain (G_d) and secrecy gain (G_c) as

$$G_d = \frac{1}{2}, \tag{3.59}$$

and

$$G_c = \frac{\sqrt{12}}{A + R_s - R_b}. \tag{3.60}$$

Remark: Based on the comparative analysis between (3.56) and (3.60) it can be noted that for $\phi = 1$ the generalized secrecy outage probability becomes classical secrecy outage probability. Also as ϕ is changed from 1 to 0 the secrecy gain improves which can be observed from (3.56).

Furthermore, to calculate the average fractional equivocation for the case when eavesdropper distance is uniform distributed we use (3.49) which is basically the expectation of fractional equivocation obtained in (3.46). This is mathematically obtained as:

$$\bar{\Delta} = \int_0^{\lambda} \frac{1}{d_E}\, dx + \int_{\lambda}^{\lambda_1} \frac{1}{d_E} \left(\frac{R_b - \ln(x) - A}{R_s} \right) dx, \tag{3.61}$$

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

$$\bar{\Delta} = \frac{\lambda}{d_E} + \left(\frac{R_b - A}{R_s d_E} \right) (\lambda_1 - \lambda) - \left(\frac{\lambda_1 \ln(\lambda_1) - \lambda_1 - \lambda \ln(\lambda) + \lambda}{R_s d_E} \right). \tag{3.62}$$

Simultaneously, the average information leakage rate (R_L) as obtained by (3.50) for the uniformly distributed eavesdropper distance is given as:

$$R_L = R_s \left(1 - \frac{\lambda}{d_E} - \left(\frac{R_b - A}{R_s d_E} \right) (\lambda_1 - \lambda) \right) + R_s \left(\frac{\lambda_1 \ln(\lambda_1) - \lambda_1 - \lambda \ln(\lambda) + \lambda}{R_s d_E} \right). \tag{3.63}$$

3.6 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 (generalized secrecy outage probability, average fractional equivocation and average information leakage rate) when the eavesdropper distance is Gaussian distributed with mean μ_x and variance σ_x^2. Now using (3.48) the expression for generalized secrecy outage probability can be derived as:

$$P_{out} = \int_{\beta}^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} \mathrm{e}^{-\frac{(d_E - \mu_x)^2}{2\sigma_x^2}}\, dx + \int_{\beta_1}^{\beta} \frac{1}{\sqrt{2\pi\sigma_x^2}} \mathrm{e}^{-\frac{(d_E - \mu_x)^2}{2\sigma_x^2}}\, dx, \tag{3.64}$$

where β_1=$e^{R_b-R_s\phi-A}$, β=e^{R_b-A} and $A = 1-\ln(\sqrt{4D\alpha})$. Similar to generalized secrecy outage probability in uniform distribution case we substitute β and β_1 in (3.64) to obtain generalized secrecy outage probability which can be written as:

$$P_{out} = Q\left(\frac{\beta-\mu_x}{\sqrt{\sigma_x^2}}\right) + Q\left(\frac{\beta_1-\mu_x}{\sqrt{\sigma_x^2}}\right) - Q\left(\frac{\beta-\mu_x}{\sqrt{\sigma_x^2}}\right). \tag{3.65}$$

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

$$P_{out} = Q\left(\frac{e^{R_b-R_s\phi-A}-\mu_x}{\sqrt{\sigma_x^2}}\right), \tag{3.66}$$

where $A = 1-\ln(\sqrt{4D\alpha})$ and $0 < \phi \leq 1$. For any value of ϕ $(0 < \phi \leq 1)$, the approximate expression for (3.66) can be obtained by using Q function approximation as given in [202]. Mathematically, the approximate expression of generalized secrecy outage probability is obtained as:

$$P_{out} \approx 1 - \frac{1}{12}e^{-\left(\frac{\gamma^2}{2}\right)} - \frac{1}{4}e^{-\left(\frac{2\gamma^2}{3}\right)}, \tag{3.67}$$

where $\gamma = \frac{e^{R_b-R_s\phi-A}-\mu_x}{\sqrt{\sigma_x^2}}$. By comparing (3.67) with

$$P_{out}^{\infty} = \left(G_c\sigma_x^2\right)^{-G_d} + O(\sigma_x^2)^{-G_d}, \tag{3.68}$$

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

$$G_d = 1, \tag{3.69}$$

and

$$G_c = \left(\frac{24}{5\left(e^{R_b-R_s\phi-A}-\mu_x\right)^2}\right). \tag{3.70}$$

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 α, 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_b.
- For a higher value of α 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 generalized secrecy outage probability reduces to classical secrecy outage which is obtained as:

$$P_{out} = \begin{cases} Q\left(\frac{e^{R_b-R_s-A}-\mu_x}{\sqrt{\sigma_x^2}}\right), & \text{for} \quad \mu_x \leq e^{R_b-R_s-A} \\ 1-Q\left(\frac{e^{R_b-R_s-A}-\mu_x}{\sqrt{\sigma_x^2}}\right), & \text{for} \quad \mu_x > e^{R_b-R_s-A}, \end{cases} \tag{3.71}$$

where $A = 1-\ln(\sqrt{4D\alpha})$. For $\mu_x > e^{R_b-R_s-A}$ case we obtain the expression for secrecy outage probability by incorporating the approximation of the Q function as given in [202], as:

$$P_{out} \approx 1 - \frac{1}{12}e^{-\left(\frac{\gamma_1^2}{2}\right)} - \frac{1}{4}e^{-\left(\frac{2\gamma_1^2}{3}\right)}, \tag{3.72}$$

where $\gamma_1 = \frac{e^{R_b-R_s-A}-\mu_x}{\sqrt{\sigma_x^2}}$. By comparing (3.72) and (3.68), the value of the diversity gain G_d and secrecy gain G_c can be obtained as:

$$G_d = 1, \tag{3.73}$$

and

$$G_c = \left(\frac{24}{5\left(e^{R_b-R_s-A}-\mu_x\right)^2}\right). \tag{3.74}$$

Remark: Based on the comparative analysis between (3.70) and (3.74) it can be noted that for $\phi = 1$ the generalized secrecy outage probability becomes classical secrecy outage probability. Also as ϕ is changed from 1 to 0 the secrecy gain improves which can be observed from (3.70).

Meanwhile, using (3.49) 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:

$$\bar{\Delta} = \int_0^{\lambda} \frac{1}{\sqrt{2\pi\sigma_x^2}} e^{-\frac{(d_E-\mu_x)^2}{2\sigma_x^2}}\, dx + \int_{\lambda}^{\lambda_1} \frac{1}{\sqrt{2\pi\sigma_x^2}} e^{-\frac{(d_E-\mu_x)^2}{2\sigma_x^2}} \left(\frac{R_b-\ln(x)-A}{R_s}\right) dx, \tag{3.75}$$

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

$$\bar{\Delta} = 1 - Q\left(\frac{\lambda - \mu_x}{\sqrt{\sigma_x^2}}\right) + \left(\frac{R_b - A}{R_s}\right)\left\{Q\left(\frac{\lambda_1 - \mu_x}{\sqrt{\sigma_x^2}}\right) - Q\left(\frac{\lambda - \mu_x}{\sqrt{\sigma_x^2}}\right)\right\}. \tag{3.76}$$

Based on the expression of average fractional equivocation the mathematical expression for average information leakage rate can be obtained from (3.50). Mathematically, average information leakage rate is written as:

$$R_L = R_s Q\left(\frac{\lambda - \mu_x}{\sqrt{\sigma_x^2}}\right) - (R_b - A)\left\{Q\left(\frac{\lambda_1 - \mu_x}{\sqrt{\sigma_x^2}}\right) - Q\left(\frac{\lambda - \mu_x}{\sqrt{\sigma_x^2}}\right)\right\}. \tag{3.77}$$

3.7 Numerical Analysis

On the basis of the mathematical analysis undertaken in the preceding section the plots between average eavesdropper capacity (C_E), the generalized secrecy outage probability (P_{out}), the average fractional equivocation ($\bar{\Delta}$) and the average information leakage rate (R_L) with respect to eavesdropper variance (σ_E^2) for uniform distribution scenario are obtained in Figure 3.3, Figure 3.4, Figure 3.5 and Figure 3.6 respectively. Simultaneously, the plots between average eavesdropper capacity (C_E), the generalized secrecy outage probability (P_{out}), the average fractional equivocation ($\bar{\Delta}$) and the average information leakage rate (R_L) with respect to eavesdropper variance (σ_E^2) for Gaussian distribution scenario are shown Figure 3.7, Figure 3.8, Figure 3.9 and Figure 3.10 respectively.

Figure 3.3 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 (σ_E^2). 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 converge. Simultaneously, with the increasing value of degradation parameter (α), the upper bound of average eavesdropper capacity further decreases. This is based on the fact that with an increase in α values, causes the rate at which the particle degrades to increase, which in turn make the information molecule to become useless.

Figure 3.4 shows the analytical and simulation behaviour of generalized secrecy outage

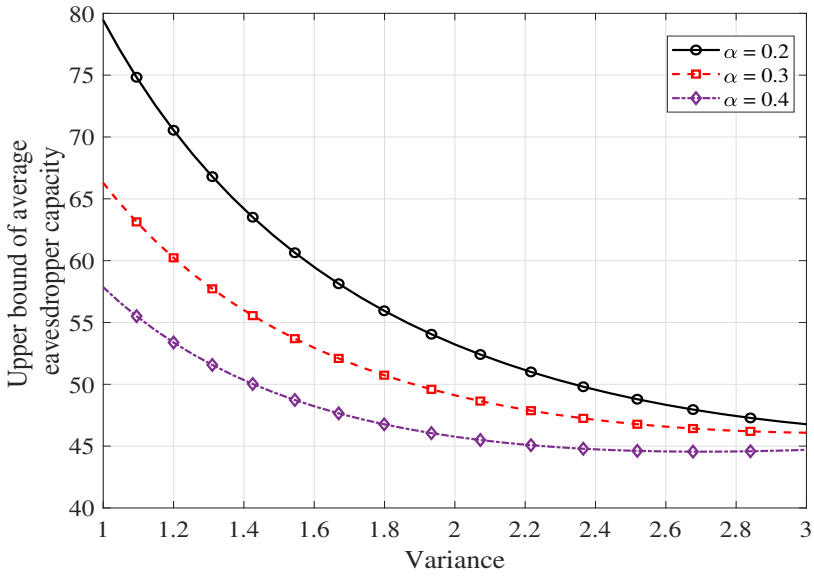

Figure 3.3: Upper bound of average eavesdropper capacity when the distance is uniform distributed RV.

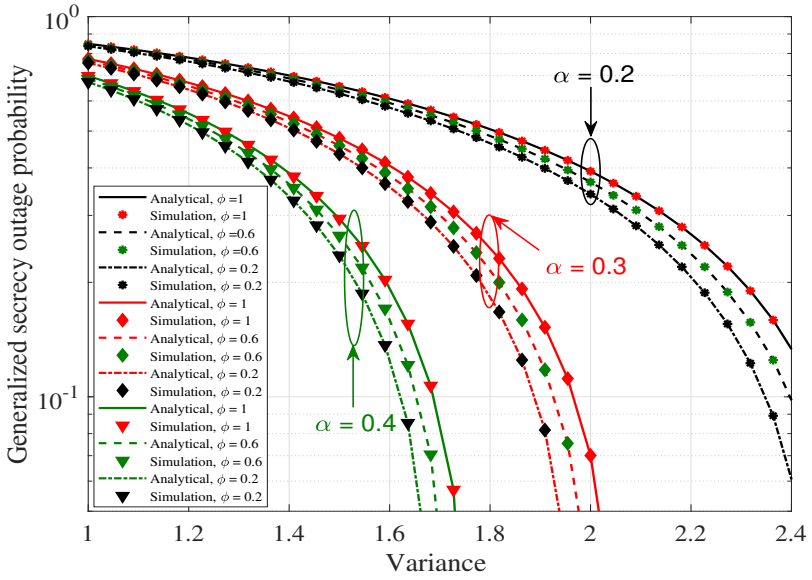

Figure 3.4: Generalized secrecy outage probability when the distance is uniform distributed RV. Here secrecy rate (R_s) is 0.1 bits/s.

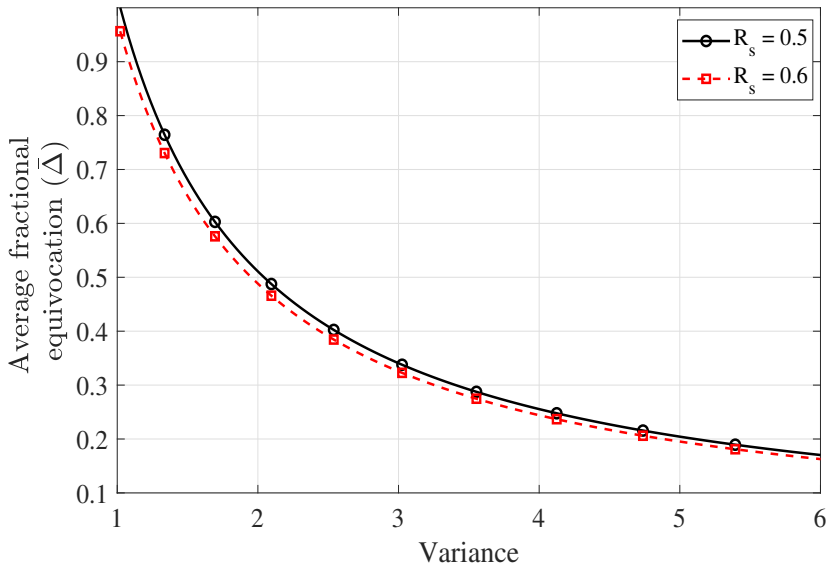

Figure 3.5: Average fractional equivocation when the distance is uniform distributed RV.

probability (P_{out}) as a function of eavesdropper variance (σ_E^2) for different values of degradation parameter (α) in the uniformly distributed scenario. Here the point to be noted that, for different α the case of $\phi = 1$ signifies the case of classical secrecy outage probability. From the figure, it can also be noted that the increasing value of the eavesdropper variance causes a sharp decay in the outage probability. This is governed by the fact that increasing variance causes an increase in secrecy capacity of the system. Moreover, increasing α cause rapid decay of the molecules, which in turn causes the outage probability to decrease. As shown in the figure, for different ϕ values, the system has different secrecy outage performance.

The variation of average fractional equivocation ($\bar{\Delta}$) with the variance of eavesdropper distance for different values of secrecy rate (R_s) in uniform distribution regime is plotted in Figure 3.5. From the figure, it can be observed that average fractional equivocation decreases as the variance of eavesdropper distance and the secrecy rate (R_s) increases, out of both the parameters the effect of increasing variance is more dominant compared to R_s. Moreover, the average fractional equivocation is non-zero even when secrecy rate (R_s) becomes zero, the expression of which can be obtained from (3.62) by putting $R_s = 0$. Moreover, $\bar{\Delta}$ increases more prominently with increase α. Thus, channel parameters play a major role in determining the secrecy performance of diffusive molecular communication systems.

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 3.6. As shown in the figure, the average information leakage rate (R_L) increase as the eavesdropper variance

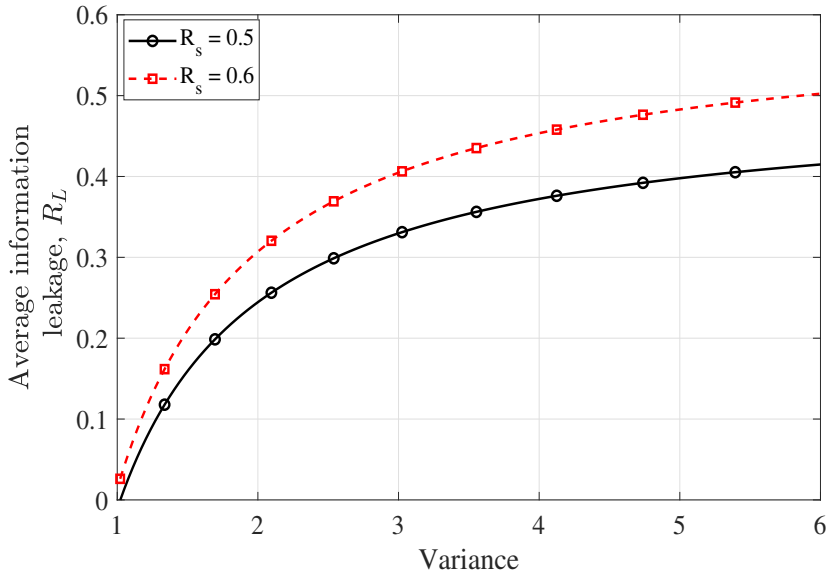

Figure 3.6: Average information leakage rate (R_L) when the distance is uniform distributed RV.

and the secrecy rate (R_s) are increased. Since R_L practically informs the amount of confidential information leaked to eavesdropper so for the higher value of variance R_L approaches to R_s. Meanwhile, increasing α causes R_L to decrease while keeping secrecy rate R_s to a particular value. This is mainly because increasing α causes the molecule to disintegrate rapidly, thereby causing the particle to be useless.

Figure 3.7 represents the plot of upper bound of average eavesdropper capacity as a function of eavesdropper variance (σ_E^2) for different values of degradation parameter (α) when the distance is Gaussian distributed. Moreover, from the figure, it is evident that for increasing values of eavesdropper variance (σ_E^2), the upper bound of average eavesdropper capacity shows a decreasing trend. Note that similar to Figure 3.3, the upper bound of average eavesdropper capacity tends to converge for higher values of variance. However, for a given eavesdropper variance (σ_E^2), the upper bound of average eavesdropper capacity decreases as α is increased from 0.2 to 0.4.

The behaviour of generalized secrecy outage probability (P_{out}) with the increasing values of the eavesdropper variance (σ_E^2) for the Gaussian distribution regime, both by analytical and simulation method, is shown in the form of a plot as depicted in Figure 3.8. Note that for different degradation parameter (α) values $\phi = 1$ represents the special case of classical secrecy outage probability. Moreover, from the figure, it can be analyzed that by increasing the variance of eavesdropper distance (σ_E^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

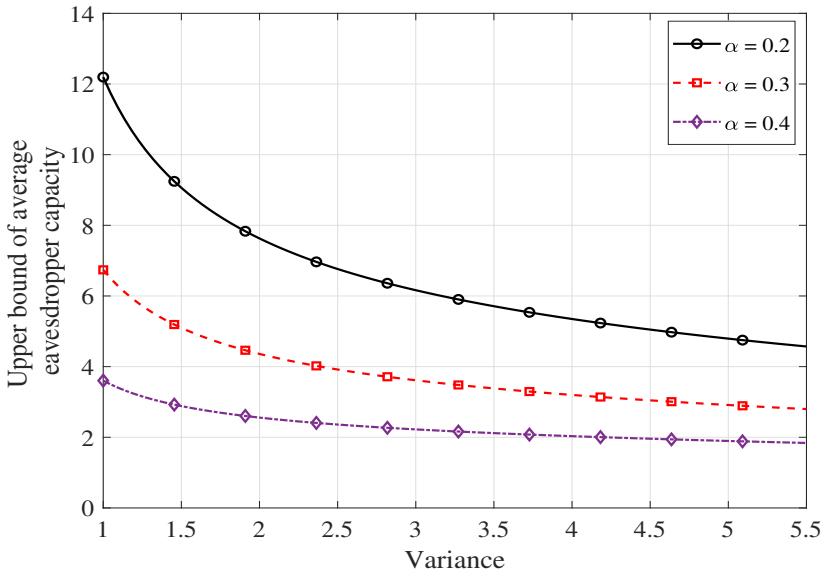

Figure 3.7: Upper bound of average eavesdropper capacity when the distance is Gaussian distributed RV.

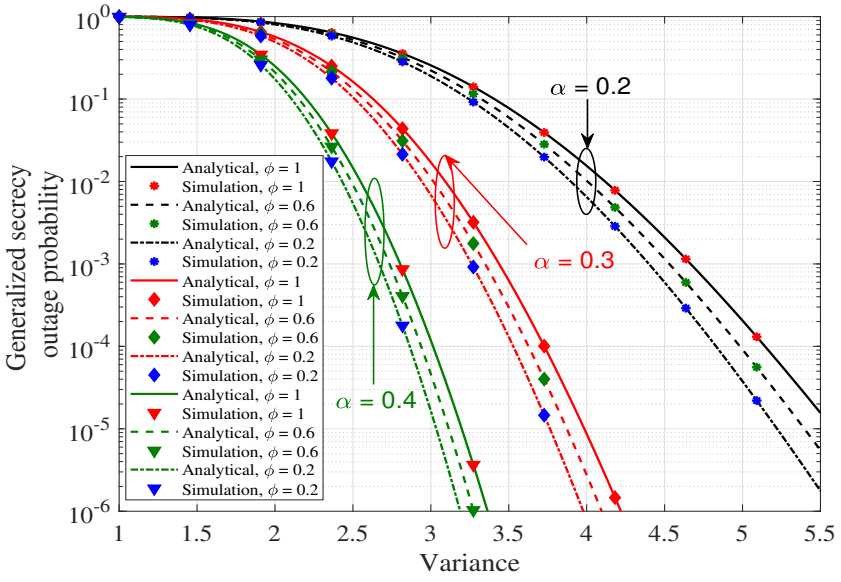

Figure 3.8: Generalized secrecy outage probability when the distance is Gaussian distributed RV. Here secrecy rate (R_s) is 0.1 bits/s.

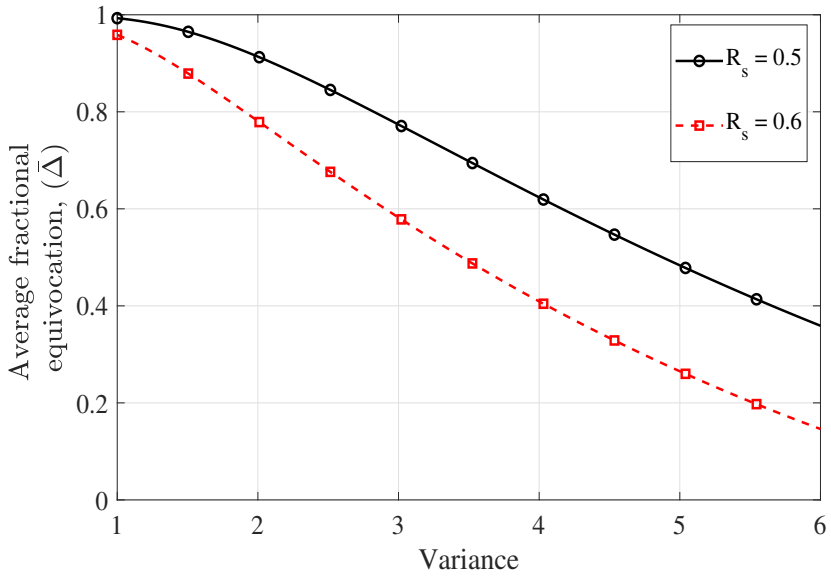

Figure 3.9: Average fractional equivocation when the distance is Gaussian distributed RV.

α causes the outage probability to decrease; this is mainly because the increasing value of α causes the molecules to degrade rapidly. Hence, this rapid decay of transmitted molecules, causes less number of molecules to reach the eavesdropper, thereby decreasing generalized secrecy outage probability.

Simultaneously, the variation of average fractional equivocation ($\bar{\Delta}$) with respect to the variance of eavesdropper distance for different values of secrecy rate (R_s) in Gaussian distribution regime is plotted in Figure 3.9. From the figure, it can be visualized that $\bar{\Delta}$ decreases simultaneously with respect to increasing variance as well as with increasing R_s. Moreover, from (3.76) even if R_s becomes zero the average fractional equivocation ($\bar{\Delta}$) is non-zero. Furthermore, simultaneous increase in the degradation parameter (α) value causes a significant increase in $\bar{\Delta}$. Thus, both channel parameters (α and R_s) play a vital role in controlling the secrecy performance of diffusive molecular communication systems.

Figure 3.10 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 R_L is always less than the R_s since the average fractional equivocation ($\bar{\Delta}$) does not become zero. Moreover, the increase in α causes R_L to decrease significantly. This is primarily because increasing α cause the particle to die out rapidly, thus failing to transmit the information.

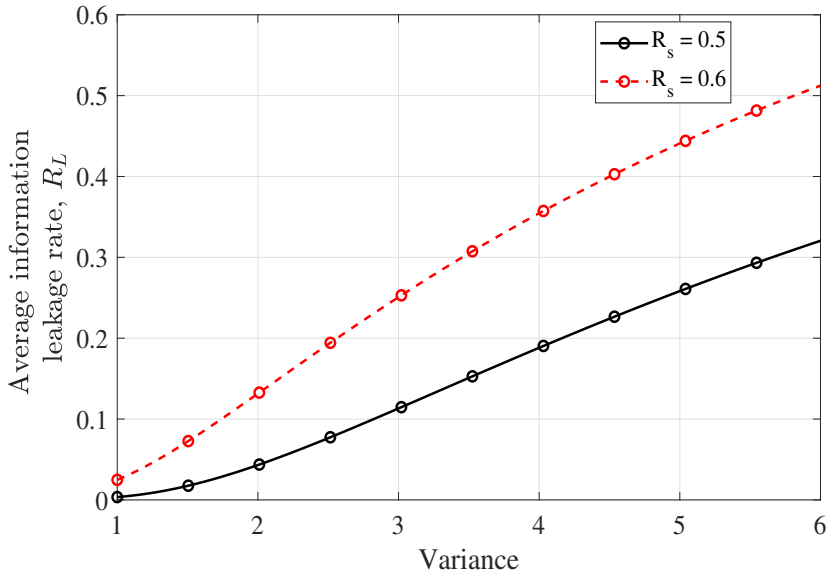

Figure 3.10: Average information leakage rate (R_L) when the distance is Gaussian distributed RV.

3.8 Summary

In this chapter, we investigated the secrecy performance of the DBMT channels when the distance of eavesdropper was assumed to be uniform and Gaussian distributed. Here, we first calculated the upper bound on the average eavesdropper capacity for both scenarios firstly when the eavesdropper distance was uniform distributed and secondly when the eavesdropper distance was Gaussian distributed. Finally, we also analyzed the secrecy of the system from the partial secrecy perspective wherein we calculated the expressions for generalized secrecy outage probability, average fractional equivocation and average information leakage rate.

Chapter 4

Single-Particle DBMT Channel Secrecy Optimization

4.1 Introduction

Based on the secrecy analysis undertaken in the previous chapter, various secrecy performance metrics are optimized in this chapter. Here we present various design parameters that would minimize GSOP, maximize average fractional equivocation, and minimize average information leakage rate, respectively. Moreover, this chapter highlights the implications of the proposed secrecy metrics on the system design. Since the impact of various secrecy metrics proposed in chapter 3 is significant from the MC perspective, it becomes imperative to study the optimization of these metrics. Moreover, optimizing various secrecy performance metrics helps in an extensive and in-depth understanding of various secrecy performance metrics and would encourage the MC theorists to undertake and manufacture various secure communication devices at the nanoscale level. Therefore, in the subsequent subsections, the optimization of various secrecy metrics is highlighted.

4.2 System Model

The transmission of information from the authorized transmitter, Alice to a legitimate receiver, Bob over a DBMT 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 is considered. Figure 4.1 represents the 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_s 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 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

$$T_a = T_t + T_n, \tag{4.1}$$

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 RV (Lévy(μ, c)) [81]. The p.d.f of Lévy distributed RV R can be represented as

$$f_R(r;\mu,c) = \sqrt{\frac{c}{2\pi(r-\mu)^3}}\exp\left(-\frac{c}{2(r-\mu)}\right), \tag{4.2}$$

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

$$c = \frac{d^2}{2D}. \tag{4.3}$$

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

$$f_{T_n}(t_n) = \frac{d}{\sqrt{4\pi D t_n^3}}\exp\left(-\frac{d^2}{4Dt_n}\right). \tag{4.4}$$

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

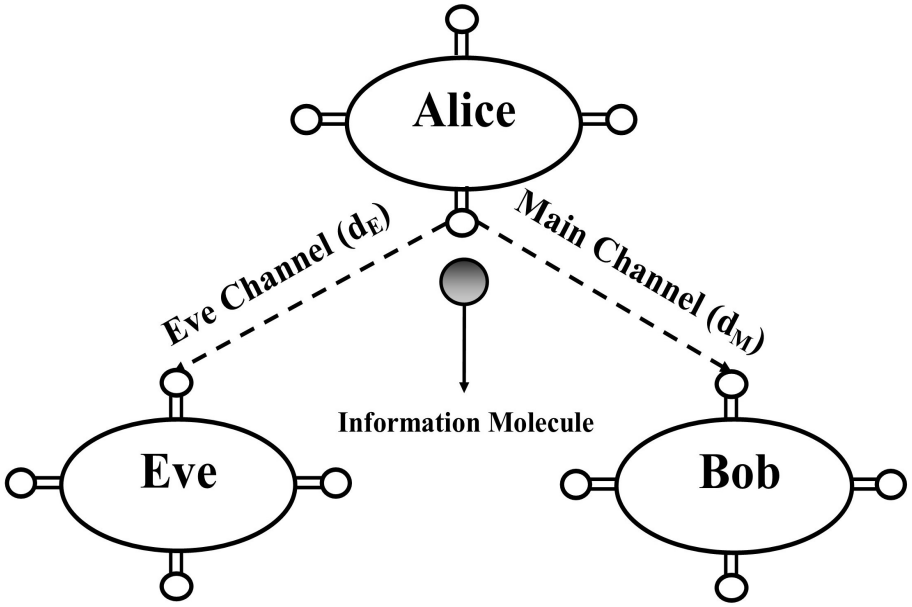

Figure 4.1: Scenario of eavesdropping in diffusion-based molecular communication.

as [80]

$$h(\tau) = \alpha e^{-\alpha\tau}, \qquad \tau > 0, \tag{4.5}$$

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 [82]

$$f_{t_d} = \begin{cases} 0, & \text{for} \quad t_d \leq 0, \\ k' \sqrt{\frac{d^2}{4\pi D t_d^3}} \mathrm{e}^{-\frac{d^2}{4Dt_d}} \mathrm{e}^{-\alpha t_d}, & \text{for} \quad t_d > 0, \end{cases} \tag{4.6}$$

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 [80], we assume that the timing channel is divided into time slots of duration τ_s. In order to avoid any ISI τ_s is taken to be *sufficiently* large. A *sufficiently* large τ_s satisfies [80, eq.(7)]

$$\tau_s \gg \tau_x + \mathbf{E}(T_n), \tag{4.7}$$

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 $p_\tau=\Pr(T_n<\tau_m)$. 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 [82, eq.(38)] is taken. Compared to the most existing literature on molecular timing channels without drift, only the authors in [82] adopt a highly realistic exponential degradation model for the lifetime of the information molecules, which well models the natural decay of the molecules [63]. 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 [82]. Mathematically the capacity upper bound is expressed as

$$C_{ub}=\max_{\tau_x} p_\tau\left(\ln(\tau_x+\tau_m)-h(T_n|L=1)\right). \tag{4.8}$$

The hitting probability of the molecule p_τ is analytically derived in [82, eq.(32)] as

$$p_\tau=k'\sqrt{\frac{c}{2\pi}}\left(2\sqrt{\frac{p}{c}}K_{1/2}(p)-\sqrt{\frac{1}{\tau_m}}K_{1/2}\left(\alpha\tau_m,\frac{c}{2\tau_m}\right)\right). \tag{4.9}$$

From [82, 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

$$C_{ub}\approx\frac{\ln(\tau_x+\tau_m)}{b}\approx\frac{\ln(\tau_s)}{b}, \tag{4.10}$$

where b is the scaling constant. Now by substituting the expression of τ_s from [80, eq.(7)] and putting $\tau_x=1$ we have,

$$\ln(\tau_s)\approx\ln\left(\tau_x+\mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{d^2}{4\alpha D}}\right)\approx\ln\left(\mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{d^2}{4\alpha D}}\right). \tag{4.11}$$

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

$$C\approx\frac{1+\ln(d)-\ln\left(\sqrt{4D\alpha}\right)}{b}. \tag{4.12}$$

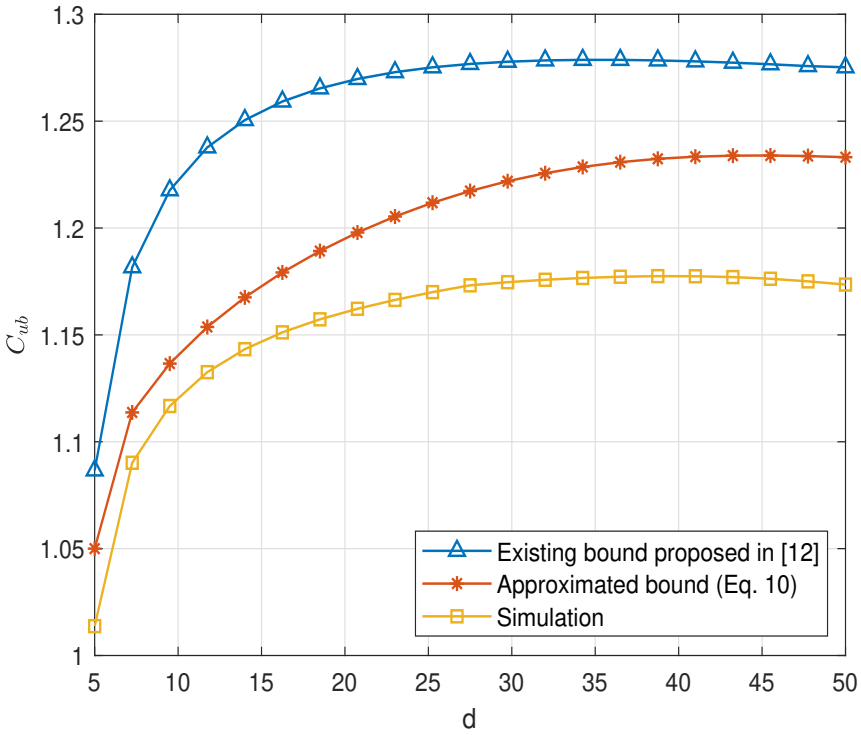

Figure 4.2: Existing [82] and proposed approximate of upper bounds on the channel capacity, along with the simulation result for parameter values of $D = 500\ \mu\text{m}^2/\text{s}$ and $\alpha = 0.01\ \text{s}^{-1}$. For all the simulation results in this chapter, we have used particle based simulations, where the results are averaged over 30,000 independent realizations of the system.

As noted in [82, 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 [82], 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 Figure 4.2 which shows the proposed approximation along with the existing expression for capacity upper bound [82, 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

$$C_B \approx \frac{1+\ln(d_M)-\ln\left(\sqrt{4D\alpha}\right)}{b}, \tag{4.13}$$

$$C_E \approx \frac{1+\ln(d_E)-\ln\left(\sqrt{4D\alpha}\right)}{b}. \tag{4.14}$$

In this work, the distances of neither Bob nor Eve are known at Alice and are assumed to be uniformly distributed. To validate the 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

$$P_{tx} = \mathbb{P}(R_B \leq C_B), \tag{4.15}$$

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 (4.15) always holds true. Using (4.13) and assuming the distance of Bob to be uniformly distributed i.e., $d_m \sim \mathscr{U}(0,\overline{d_M})$, the expression (4.15) is modified as

$$P_{tx} = \mathbb{P}\left(R_B \leq \frac{A+\ln(d_M)}{b}\right) = \mathbb{P}(d_M \geq \mathrm{e}^{R_B b - A}), \tag{4.16}$$

where $A = 1-\ln(\sqrt{4D\alpha})$. Using probability definition the expression (4.16) can be modified to be written as

$$P_{tx} = \int_{\mathrm{e}^{R_B b-A}}^{\overline{d_M}} \frac{1}{\overline{d_M}} dx = 1 - \frac{\mathrm{e}^{R_B b-A}}{\overline{d_M}}. \tag{4.17}$$

4.3 Secure Transmission Design

In this section, we optimize the secrecy performance of the system described in the previous section. 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 chapter, 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 chapter.

The expression for the GSOP is given by

$$P_{out} = \mathbb{P}(\Delta < \phi), \tag{4.18}$$

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 ($\mathscr{U}(0, \overline{d_E})$) is given by

$$\begin{aligned} P_{out} &= \mathbb{P}(d_E \geq \mathrm{e}^{R_B b - A}) + \mathbb{P}(\mathrm{e}^{R_B b - R_S b - A} < d_E < \mathrm{e}^{R_B b - A}) \\ &\quad .\mathbb{P}\left(\frac{R_B b - \ln(d_E) - A}{R_S} < \phi \,\middle|\, \mathrm{e}^{R_B b - R_S b - A} < d_E < \mathrm{e}^{R_B b - A}\right) \\ &= 1 - \frac{\mathrm{e}^{R_B b - R_S \phi - A}}{\overline{d_E}}. \end{aligned} \tag{4.19}$$

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

written as

$$\begin{aligned} \underset{R_B,R_S}{\text{minimize}} \quad & P_{out} = 1 - \frac{\mathrm{e}^{R_B b - R_S \phi - A}}{\overline{d_E}}, \\ \text{subject to} \quad & \eta \geq \Gamma,\ R_B \geq R_S > 0. \end{aligned} \tag{4.20}$$

The average fractional equivocation is given as

$$\bar{\Delta} = \mathbb{E}(\Delta). \tag{4.21}$$

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

$$\bar{\Delta} = \int_0^{\lambda} \frac{1}{d_E}\, dx + \int_{\lambda}^{\lambda_1} \frac{1}{d_E} \left(\frac{R_B b - \ln(x) - A}{R_S} \right) dx. \tag{4.22}$$

This results in

$$\bar{\Delta} = \frac{\lambda}{\overline{d_E}} + \left(\frac{R_B b - A}{R_S b \overline{d_E}} \right) (\lambda_1 - \lambda) - \left(\frac{\lambda_1 \ln(\lambda_1) - \lambda_1 - \lambda \ln(\lambda) + \lambda}{R_S b \overline{d_E}} \right), \tag{4.23}$$

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 $\eta \geq \Gamma$ and $R_B \geq R_S > 0$ can be expressed as

$$\begin{aligned} \underset{R_B,R_S}{\text{maximize}} \quad & \frac{\lambda}{\overline{d_E}} + \left(\frac{R_B b - A}{R_S b \overline{d_E}} \right) (\lambda_1 - \lambda) - \frac{\lambda_1 \ln(\lambda_1)}{R_S b \overline{d_E}} \\ & + \frac{\lambda_1}{R_S b \overline{d_E}} + \frac{\lambda \ln(\lambda)}{R_S b \overline{d_E}} - \frac{\lambda}{R_S b \overline{d_E}}, \\ \text{subject to} \quad & \eta \geq \Gamma, R_B \geq R_S > 0. \end{aligned} \tag{4.24}$$

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

$$R_L = \mathbb{E}\{(1-\Delta)R_S\} = (1-\bar{\Delta})R_S. \tag{4.25}$$

Using (4.23), the average information leakage rate R_L for the case when Eve's distance is uniformly distributed simplifies to

$$R_L = R_s - \frac{\lambda\,(R_s b + \ln(\lambda) - R_B b + A - 1)}{b\overline{d_E}} - \frac{\lambda_1\,(R_B b - \ln(\lambda_1) - A + 1)}{b\overline{d_E}}. \tag{4.26}$$

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

$$\begin{aligned} \underset{R_B,R_S}{\text{minimize}} \quad & R_s - \frac{\lambda\left(R_s b + \ln(\lambda) - R_B b + A - 1\right)}{b\overline{d_E}} \\ & - \frac{\lambda_1\left(R_B b - \ln(\lambda_1) - A + 1\right)}{b\overline{d_E}}. \\ \text{subject to} \quad & \eta \geq \Gamma,\ R_B \geq R_S > 0. \end{aligned} \tag{4.27}$$

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

$$\eta = R_S - \frac{R_S \mathrm{e}^{R_B b - A}}{\overline{d_M}}, \tag{4.28}$$

the optimization problem in (4.27) can be reformulated as

$$\begin{aligned} \underset{R_B,R_S}{\text{maximize}} \quad & R_S - \frac{R_S \mathrm{e}^{R_B b - A}}{\overline{d_M}}. \\ \text{subject to} \quad & R_B \geq R_S > 0. \end{aligned} \tag{4.29}$$

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 (4.29) becomes

$$\begin{aligned} \underset{R_S}{\text{maximize}} \quad & R_S - \frac{R_S \mathrm{e}^{R_S b - A}}{\overline{d_M}}. \\ \text{subject to} \quad & R_S > 0. \end{aligned} \tag{4.30}$$

Taking the partial derivative of (4.30) w.r.t. R_S, we get

$$\frac{\partial\eta}{\partial R_S} = 1 - \frac{\mathrm{e}^{R_S b - A}}{\overline{d_M}} - \frac{b R_S \mathrm{e}^{R_S b - A}}{\overline{d_M}}. \tag{4.31}$$

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

$$R_S^{\square} = \frac{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right) - 1}{b}, \tag{4.32}$$

where $\mathrm{W}_0(\cdot)$ denotes the principal branch of the Lambert W function. Substituting (4.32) in

(4.30), the range of the throughput can be obtained as

$$0 \leq \eta \leq \left(\frac{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right)-1}{b} \right) \left(1 - \frac{\mathrm{e}^{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right)-1-A}}{\overline{d_M}} \right). \tag{4.33}$$

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 $R_{s,min} \leq R_S \leq R_{s,max}$. Moreover, the optimum value of Bob's rate for which the throughput of the system is maximized can be obtained from (4.29) and is given by

$$R_B^* = \frac{1}{b}\left(A + \ln\left(\overline{d_M} - \frac{\overline{d_M}\eta_{max}}{R_S^*} \right) \right), \tag{4.34}$$

where η_{max} is expressed as

$$\eta_{max} = \left(\frac{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right)-1}{b} \right) \left(1 - \frac{\mathrm{e}^{\mathrm{W}_0\left(\overline{d_M}\mathrm{e}^{A+1}\right)-1-A}}{\overline{d_M}} \right). \tag{4.35}$$

This R_B^* is different for different R_S^*. Now, according to (4.20), in order to minimize the GSOP, we need to maximize

$$F_1 = R_B b - R_S \phi - A. \tag{4.36}$$

Therefore, by substituting (4.34) in (4.36) and differentiating w.r.t. R_S, we get

$$\phi = \frac{\overline{d_M}\eta_{max}}{R_S\left(\overline{d_M}R_S - \overline{d_M}\eta_{max}\right)}. \tag{4.37}$$

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

$$R_{s1}^* = \frac{\eta_{max}\phi + \sqrt{\eta_{max}^2\phi^2 + 4\phi\eta_{max}}}{2\phi}. \tag{4.38}$$

Thus, Bob's optimal rate R_{B1}^* can be obtained by substituting (4.38) in (4.34). Similarly, the optimal secrecy rate R_{s2}^* and Bob's optimal rate R_{B2}^* which maximize the average fractional equivocation $\bar{\Delta}$, subject to $R_{s,min} \leq R_S \leq R_{s,max}$ can be obtained after solving the maximization

problem as given in (4.24). The optimization problem in (4.24) can be rewritten as

$$\begin{aligned} \underset{R_S}{\text{maximize}} \quad & \frac{e^{R_B b - A}\left(1 - e^{-R_S b}\right)}{b R_S \overline{d_E}}. \\ \text{subject to} \quad & R_{s,min} \leq R_S \leq R_{s,max}. \end{aligned} \tag{4.39}$$

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

$$F_2 = \frac{e^{R_B b - A}\left(1 - e^{-R_S b}\right)}{b R_S \overline{d_E}}. \tag{4.40}$$

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 (4.34). By putting R_{B2}^* in (4.39), the optimization problem which maximizes the average fractional equivocation $\bar{\Delta}$ subject to $R_{s,min} \leq R_S \leq R_{s,max}$ can be modified as

$$\begin{aligned} \underset{R_S}{\text{maximize}} \quad & \frac{\left(\overline{d_M} R_S - \overline{d_M}\eta_{max}\right)\left(1 - e^{-R_S b}\right)}{b R_S^2 \overline{d_E}}. \\ \text{subject to} \quad & R_{s,min} \leq R_S \leq R_{s,max}. \end{aligned} \tag{4.41}$$

From (4.41), 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 (4.27), 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.

4.4 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

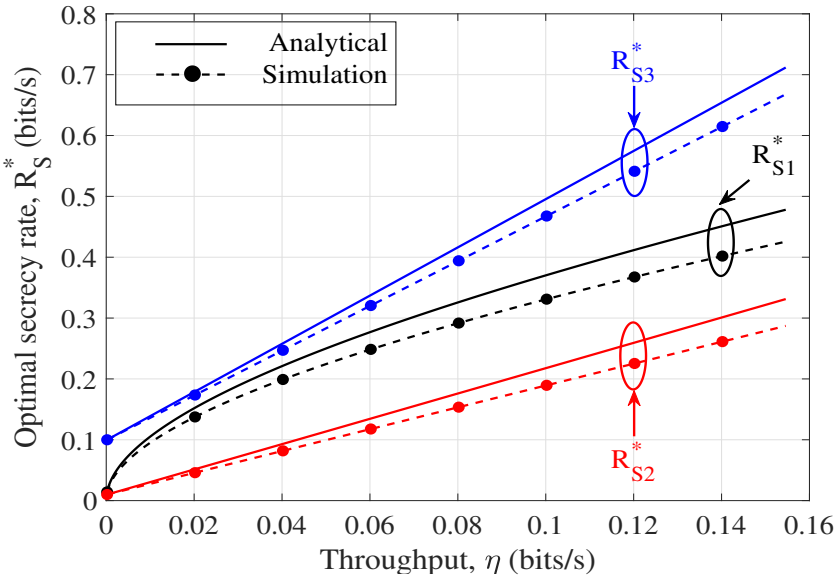

Figure 4.3: Optimal secrecy rate versus throughput for different secrecy performance metrics. The other parameters are $\phi = 1$, $\overline{d_M} = 50\ \mu$m and $\overline{d_E} = 50\ \mu$m.

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 (4.33) is $0 \leq \eta \leq 0.16$ bits/s with $\alpha = 0.01s^{-1}$ and D=500$\mu m^2/s$. Using the η range, we first analyze the optimal secrecy rate that optimizes various secrecy performance metrics.

Figure 4.3 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 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 (4.34) 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.

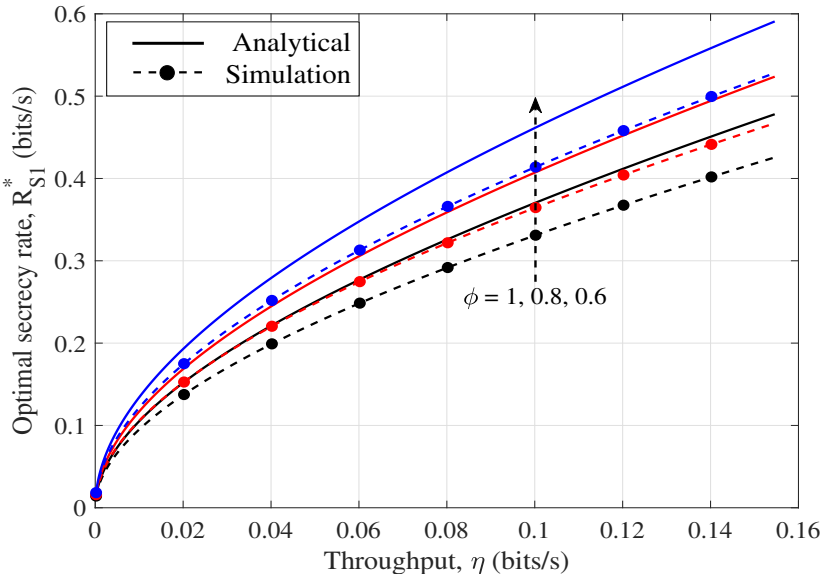

Figure 4.4: Optimal secrecy rate versus throughput for GSOP for different fractional equivocation (ϕ). The other parameters are $\overline{d_M} = 50\ \mu$m and $\overline{d_E} = 50\ \mu$m.

The variation of optimal secrecy rate, R^*_{s1}, which basically minimizes the GSOP, is shown in Figure 4.4 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 Figure 4.5. It can be observed from the GSOP plot that increasing the throughput constraint increases the GSOP 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.

Figure 4.6 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 that though the transmission with R^*_{B2} and R^*_{s2} maximizes average fractional

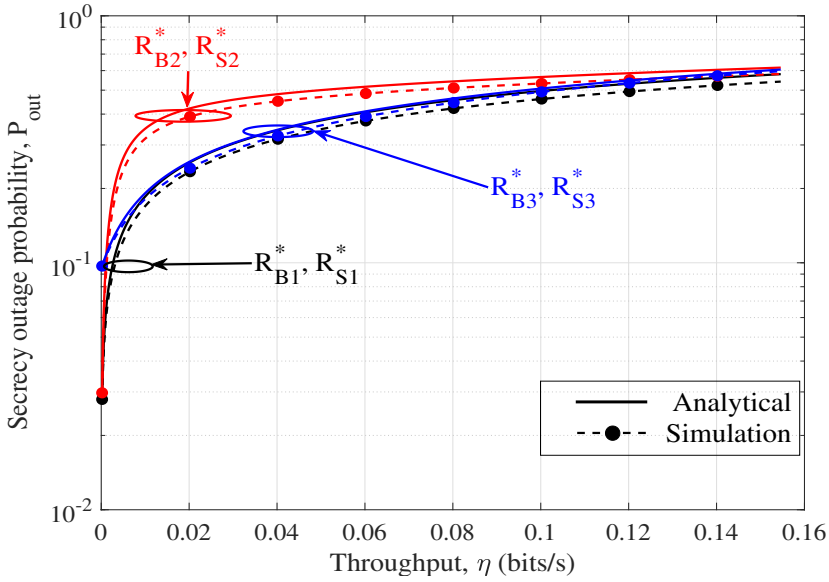

Figure 4.5: Secrecy outage probability versus throughput. The other parameters are $\phi = 1$, $\overline{d_M} = 50$ μm, and $\overline{d_E} = 50$ μm.

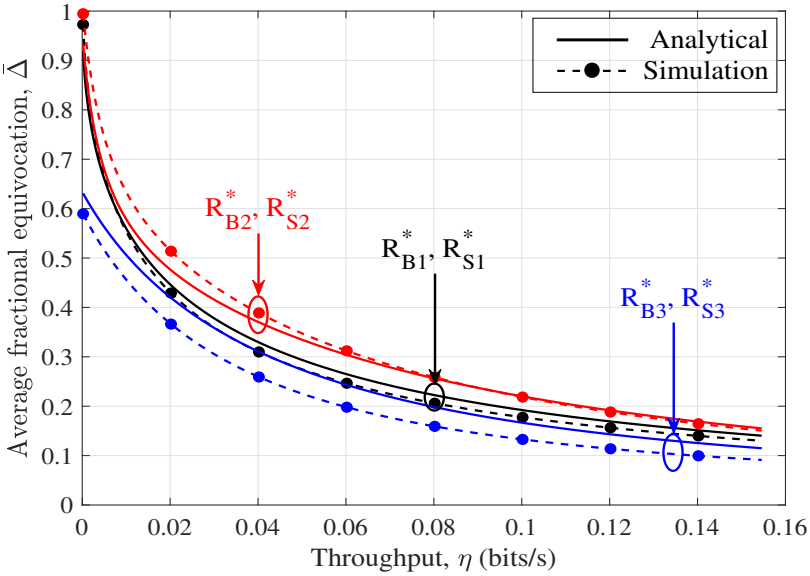

Figure 4.6: Average fractional equivocation versus throughput. The other parameters are $\phi = 1$, $\overline{d_M} = 50$ μm, and $\overline{d_E} = 50$ μm.

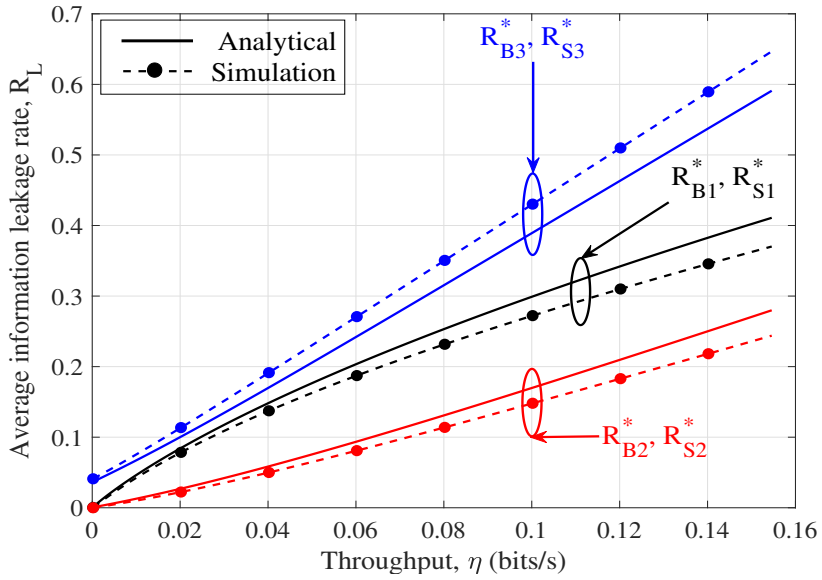

Figure 4.7: Average information leakage rate versus throughput. The other parameters are $\phi = 1$, $\overline{d_M} = 50\ \mu$m, and $\overline{d_E} = 50\ \mu$m.

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 Figure 4.7. 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 Figure 4.5, Figure 4.6 and Figure 4.7 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.

4.5 Summary

In this chapter, we obtained various optimal rate parameters which minimizes GSOP, maximizes average fractional equivocation and minimizes the average information rate of the DBMT channels. For obtaining the optimal rate parameters which would be an useful design parameters for designing a secure DBMT channel we first calculated the maximum throughput of the system. Using the maximum throughput constraint we then calculated the optimal rate parameters expressions for different design setup. Finally, from the numerical results it could 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.

Chapter 5

Secrecy From Amount Of Confusion Level Perspective

5.1 Introduction

In this chapter, we study the secrecy performance of the multi-particle DBMT channels from the amount of confusion level perspective. Here we use the second-order statistics to analyze secrecy in diffusive molecular timing channels. For this, we first derive the expressions of the first order secrecy performance metrics such as the GSOP, the average fractional equivocation and the average information leakage rate. Using the expressions of GSOP and average fractional equivocation in this chapter, the analysis regarding the amount of confusion level is presented for a DBMT channel. The amount of confusion level being a second-order metric is analogous to the amount of fading metric employed in the wireless communication scenario and signifies the level at which Eve is confused. Finally, from the amount of confusion level analysis, useful insights about the system's secrecy performance are measured in this chapter.

5.2 System Model

We consider a one-dimensional (1D) environment where the authorized transmitter, Alice, is located between the legitimate receiver, Bob, and the eavesdropper, Eve. Alice sends confidential information to an intended receiver, Bob over a diffusive moleculer timing (DBMT) channel, where the information to be transmitted is encoded in the time of release of the information molecules. Figure 5.1 represents the eavesdropping scenario under consideration. Similar to

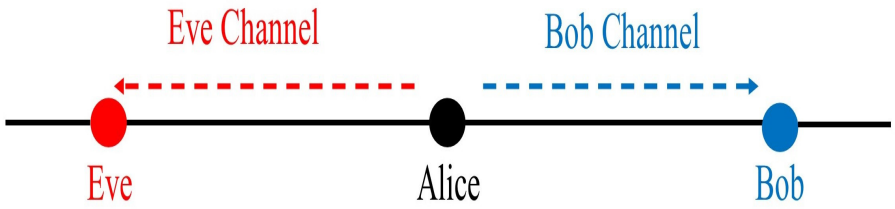

Figure 5.1: Scenario of eavesdropping in diffusive molecular timing channels [203].

approach taken in the previous models in this chapter also the Alice is considered as a point source that can release an impulse of N identical, finite lifetime, molecules in to the aqueous media forming the MC channel. Each of the transmitted molecules follows an independent and identically distributed (iid) path to the either Bob or Eve. Both Bob and Eve are assumed to be fully absorbing receivers. In this work, the distance from Alice to Bob and Eve, respectively, is assumed to be sufficiently large such that Bob and Eve does not impact each other in terms of the number of molecules received [203]. Furthermore, the fluid media is assumed to be free from any drift. Alice, Bob and Eve are assumed to be perfectly time-synchronized, i.e., Alice perfectly controls the time of release of the information molecules, while both Bob and Eve and can perfectly measure the arrival time of the information molecules. Time synchronization is needed to ensure the orderly arrival of the information molecules and to prevent disruption of the system. The orderly arrival of the particles results in identical and independent successive channel usage. The time synchronization in MC is needed in a variety of biosensor network and data gathering applications such as the release of anti-body molecules and the interpretation of sensed data[204]. In many practical scenarios, primarily in Blackhole and Sentry attacks, there is a requirement for Eve's clock synchronization in order to attract the information molecules towards it. In both the scenarios, the cooperative nature of Eve enables time synchronization leading to the emission of certain chemical attractants only after Alice has transmitted the information molecules.

To characterize the DBMT channel, let T_x represent the time at which N molecules are released by the transmitter. Each molecule released then follows a random independent propagation path and arrives at the receiver at a time T_y. This arrival time is the sum of T_x and random propagation delay T_n. Mathematically, the arrival time for molecules received at Bob (B) or Eve (E) is given as

$$T_{y_k} = T_x + T_{n_k}, \tag{5.1}$$

where $k \in \{Bob, Eve\}$.

In our case, where the fluid media is free of any drift, the random propagation time T_n is a Lévy distributed RV (Lévy(μ, c)) [81]. Here μ is the location parameter and $c = \frac{d^2}{2D}$ is the Lévy noise parameter. Note that d is the distance travelled by the information molecule from Alice, and D is the diffusion coefficient. Furthermore, the information molecules are assumed to have an exponentially decaying life expectancy that is modeled as[205]

$$h(\tau_n) = \alpha e^{-\alpha \tau_n}, \qquad \tau_n > 0, \tag{5.2}$$

where α is the *degradation parameter* and τ_n represents the *lifetime of the information molecule*. This finite life time of the information molecules allows us to represent the random propagation time as the truncated Lévy distribution [82]

$$f_{t_d} = \begin{cases} 0, & \text{for} \quad t_d \leq 0 \\ \mathrm{e}^{p} \sqrt{\frac{d^2}{4\pi D t_d^3}} \mathrm{e}^{-\frac{d^2}{4Dt_d}} \mathrm{e}^{-\alpha t_d} & \text{for} \quad t_d > 0, \end{cases} \tag{5.3}$$

where p is the scaled version of the noise parameter given by $p{=}\sqrt{2\alpha c}$.

Note that the finite life expectancy of the information molecules allows us to consider the MC channel free of inter-symbol interference (ISI) for our analysis. Taking an approach similar to [82], let τ_m be the time taken by the information molecule to decay to $Z\%$ of its initial value. After $Z\%$ of degradation, the molecules are not recognizable by the receiver and do not contribute to the ISI if the time slot for each transmission is made *sufficient* large. In this case each time slot τ_s satisfies $\tau_s = \tau_x + \tau_m$, where τ_x represents the symbol interval in which the molecules are transmitted.

Figure 5.2 represents this multi-particle DBMT channel. From the figure, it is evident that if the random propagation time (T_n) is more than τ_m, the information molecule is assumed to be unrecognizable at the receiver (either Bob or Eve) and therefore, no information is conveyed. These molecules are then removed from the environment through certain chemical reactions. For example, Acetylcholine molecules used in neuromuscular synapses to trigger muscle contraction are removed from the environment using Acetylcholinesterase enzymes. Let N be the number of identical particles transmitted by Alice at a particular instant T_x. The number of molecules released by Alice is assumed to be the same for all the transmissions. Furthermore, let M_B and M_E be the number of molecules out of the N transmitted information molecules arriving at Bob and Eve within a time slot, respectively. Let p_τ denotes the hitting probability

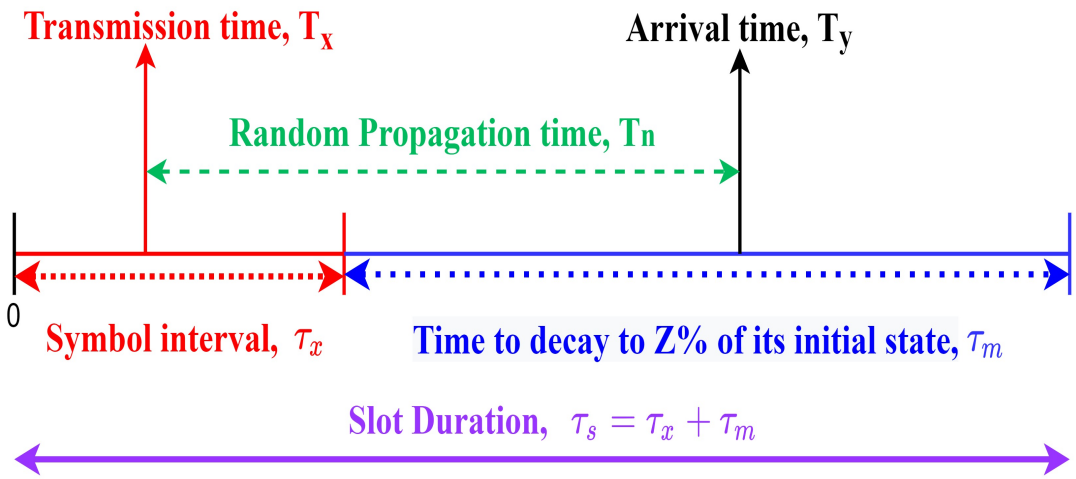

Figure 5.2: Diffusive molecular timing channels.

of an information molecule [82, eq.(32)]

$$p_\tau = \mathrm{e}^p \sqrt{\frac{c}{2\pi}} \left(2\sqrt{\frac{p}{c}} K_{1/2}(p) - \sqrt{\frac{1}{\tau_m}} K_{1/2}\left(\alpha\tau_m, \frac{c}{2\tau_m} \right) \right). \tag{5.4}$$

Using this formulation, an existing upper bound on the capacity of the molecular timing channel as given by [82, eq.(55)] is

$$C_{ub} = \max_{\tau_x} \frac{2\ln(\tau_s) - \ln(2\pi\mathrm{e}/M^2\alpha^2)}{2\ln(2)(\tau_x + \tau_m)}. \tag{5.5}$$

This can be further simplified as

$$C_{ub} = \max_{\tau_x} \frac{2\ln(M) + B}{A}, \tag{5.6}$$

where $A = 2\ln(2)(\tau_s)$ and $B = 2\ln(\tau_s) - \ln(2\pi e/\alpha^2)$ respectively. Simultaneously, for the sake of distinguishing, the Bob channel capacity is represented as C_B while the Eve channel capacity is represented by C_E. Mathematically, the expressions for channel capacities in terms of the number of molecules received in that time slot are given by

$$C_B = \max_{\tau_x} \frac{2\ln(M_B) + B}{A}, \tag{5.7}$$

$$C_E = \max_{\tau_x} \frac{2\ln(M_E) + B}{A}. \tag{5.8}$$

In this work, the number of molecules received at Eve (M_E) are neither known at Alice nor at

Bob. Considering that Alice transmits a large number of molecules, the number of molecules arriving at Eve can be assumed to be Gaussian distributed ($\mathscr{N}(Np_\tau, Np_\tau(1-p_\tau))$).

5.3 Secrecy Performance Metrics

In this section, we focus on deriving the analytical expressions for the secrecy metrics of the considered multi-particle DBMT channel. Due to the unavailability of instantaneous CSI of either Bob or Eve at Alice, it becomes difficult to achieve exact expressions for the channel secrecy. For such an environment, the secrecy outage probability (SOP) can be a valuable metric to characterize the secrecy performance. However, SOP being the first-order measure, has certain limitations, especially in terms of decoding error probability of Eve. Furthermore, the classical SOP neither gives information regarding the rate at which the confidential information is leaked to Eve nor gives any insight into Eve's level of confusion. Therefore, to overcome the limitations mentioned above and to analyze the secrecy of the system from the partial secrecy perspective, we use metrics such as generalized secrecy outage probability (GSOP), average fractional equivocation ($\bar{\Delta}$), and average information leakage rate (R_L). Moreover, we propose a new second-order secrecy metric, namely the amount of confusion level (ACL), which primarily quantifies the severity of confusion level at the eavesdropping user. This new secrecy metric, along with other mentioned metrics, will help to gain valuable insights into the dynamics of the secrecy performance of the system and would, in turn, be helpful for the designer to analyze how information integrity is maintained in MC when Eve's instantaneous CSI is unavailable at Bob.

5.3.1 Generalized Secrecy Outage Probability

In practical systems where partial secrecy is usually experienced, the GSOP analysis is employed by undertaking fractional equivocation (Δ). Mathematically, Δ is usually denoted as [199, eq.(3)]. Fractional equivocation is associated with the decoding error probability and is primarily dependent on coding and transmission strategies.

In our analysis, confidential information, M, is encoded into a n-vector X^n. Further, we consider two rate parameters, i.e., transmission rate, $R_B = \frac{H(X^n)}{n}$, and confidential information rate $R_S = \frac{H(M)}{n}$, where $H(X^n)$ is entropy of encoded n-vector X^n and $H(M)$ is entropy of the source information. A length n wiretap code is constructed by generating 2^{nR_B} codewords $x^n(w,v)$,

where $w = 1,2,...,2^{nR_S}$ and $v = 1,2,...,2^{n(R_B-R_S)}$. Foe each message index w, we randomly select v from $\{1,2,...,2^{n(R_B-R_S)}\}$ with uniform probability and transmit the codeword $x^n(w,v)$. To reduce system complexity, a fixed-rate transmission scheme is considered. Therefore, R_B and R_S are assumed to be constant over time. Fixed R_B selection is based on the transmission probability given as $\mathbb{P}(R_B \leq C_B)$. Using C_E from (5.8), the expression for fractional equivocation becomes

$$\Delta = \begin{cases} 1, & \text{for } M_E \leq \mathrm{e}^{\frac{A(R_B-R_S)-B}{2}} \\ \frac{AR_B-2\ln(M_E)-B}{AR_S}, & \text{for } \mathrm{e}^{\frac{A(R_B-R_S)-B}{2}} < M_E < \mathrm{e}^{\frac{AR_B-B}{2}} \\ 0, & \text{for } \mathrm{e}^{\frac{AR_B-B}{2}} \leq M_E, \end{cases} \tag{5.9}$$

where $\mathrm{e}^{\frac{A(R_B-R_S)-B}{2}} = \lambda_1$ and $\mathrm{e}^{\frac{AR_B-B}{2}} = \lambda_2$. Using fractional equivocation expression, the expression for GSOP is given as

$$P_{out} = \mathbb{P}(\Delta < \phi), \tag{5.10}$$

where ϕ is the minimum value of fractional equivocation ($0 < \phi < 1$). Thus the expression for generalized SOP when the number of molecules received by Eve is Gaussian distributed ($\mathcal{N}(Np_\tau, Np_\tau(1\text{-}p_\tau))$) is given by

$$\begin{aligned} P_{out} &= \mathbb{P}(M_E \geq \lambda_2) + \mathbb{P}(\lambda_1 < M_E < \lambda_2) \\ &\quad \times \mathbb{P}\left(\frac{AR_B - 2\ln(M_E) - B}{AR_S} < \phi \,\middle|\, \lambda_1 < M_E < \lambda_2\right) \\ &= Q\left(\frac{\mathrm{e}^{\frac{A(R_B-R_S\phi)-B}{2}} - \mu_M}{\sigma_M}\right). \end{aligned} \tag{5.11}$$

Proof: The detailed proof is given in Appendix A.

Remark 1: Note that for $\phi = 1$ the GSOP reduces to classical SOP. Further, for higher c values and fixed α, the outage probability $P_{out} \to 0$. To observe this, we first note that for higher c, the hitting probability of molecule $p_\tau \to 0$, and thus, the outage probability approaches zero. This can be formally verified by writing P_{out}, for higher c as

$$P_{out} = \lim_{p_\tau \to 0} Q\left(\frac{\mathrm{e}^{\frac{A(R_B-R_S\phi)-B}{2}} - \mu_M}{\sigma_M}\right) = 0. \tag{5.12}$$

Practically, increasing c signifies an increase in the distance of Eve from Alice severely affecting the Eve channel quality. The deterioration in Eve channel quality leads to improvement in the

secrecy performance of the system.

Remark 2: For larger values of R_S, the outage probability P_{out} of (5.11) becomes

$$P_{out} = \lim_{R_S \to \infty} Q\left(\frac{e^{\frac{A(R_B - R_S\phi) - B}{2}} - \mu_M}{\sigma_M}\right) = 1. \tag{5.13}$$

Remark 3: For high values of α and fixed c the hitting probability of molecule, $p_\tau \to 0$. Hence, when $p_\tau \to 0$ then according to (5.11) the expression for outage probability becomes

$$P_{out} = \lim_{p_\tau \to 0} Q\left(\frac{e^{\frac{A(R_B - R_S\phi) - B}{2}} - \mu_M}{\sigma_M}\right) = 0. \tag{5.14}$$

In practical scenarios, the degradation process can be enhanced by introducing certain enzymes or molecules. This acceleration in the degradation process makes the molecules unable to be absorbed by Eve, thereby improving secrecy.

5.3.2 Average Fractional Equivocation

The average fractional equivocation ($\bar{\Delta}$) gives the asymptotic bound on the decoding error probability of Eve. The expression for $\bar{\Delta}$ is obtained as

$$\begin{aligned}\bar{\Delta} = \mathbb{E}(\Delta) = &\int_0^{\lambda_1} \frac{1}{\sqrt{2\pi\sigma_M^2}} e^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm + \int_{\lambda_1}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} e^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \left(\frac{AR_B - B}{AR_S}\right) dm \\ &- \int_{\lambda_1}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} e^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \left(\frac{2\ln(m)}{AR_S}\right) dm.\end{aligned} \tag{5.15}$$

Upon further simplification, an analytical expression for $\bar{\Delta}$ is obtained as

$$\begin{aligned}\bar{\Delta} \approx 1 - Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) + \left(\frac{AR_B - B}{AR_S}\right)\left\{Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2 - \mu_M}{\sigma_M}\right)\right\} \\ - \frac{2(a(\mu_M)^{\frac{1}{a}} - a)}{AR_S}\left\{Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2 - \mu_M}{\sigma_M}\right)\right\}.\end{aligned} \tag{5.16}$$

Proof: The detailed proof is given in Appendix B.

Remark 4: Note that for high c value, the hitting probability of molecules becomes zero

making the argument $\frac{\mu_M}{\sigma_M}$ inside the Q function to approach zero. Therefore, $\bar{\Delta}$ in (5.16) becomes

$$\bar{\Delta} \approx \left(1 - Q\left(\frac{\mu_M}{\sigma_M}\right)\right) \rightarrow (1 - Q(0)) \rightarrow 0.5. \tag{5.17}$$

Note that for lower and mid range c values ($c < 20$) the $\bar{\Delta}$ approaches 1 but for high c values it starts to converge towards 0.5.

Remark 5: For larger values of R_S, $\bar{\Delta}$ becomes independent of μ_M and σ_M. Clearly, for large R_S the expression $\frac{\lambda_1 - \mu_M}{\sigma_M}$ approaches $\frac{-\mu_M}{\sigma_M}$ which leads $\bar{\Delta}$ to converges to

$$\bar{\Delta} \approx 1 - Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{-\mu_M}{\sigma_M}\right) \rightarrow 0. \tag{5.18}$$

Remark 6: For higher degradation, the hitting probability (p_τ) of molecule decreases. Further, for high α value the argument inside the Q function becomes $\frac{\lambda_1 - \mu_M}{\sigma_M} \rightarrow \infty$. Meanwhile, with a decrease in p_τ the argument $\frac{\mu_M}{\sigma_M}$ approaches zero. Hence, $\bar{\Delta}$ in (5.16) becomes

$$\bar{\Delta} \approx \left(1 - Q\left(\frac{\mu_M}{\sigma_M}\right)\right) \rightarrow (1 - Q(0)) \rightarrow 0.5. \tag{5.19}$$

5.3.3 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 is leaked to eavesdropper is defined as the average information leakage rate. Using average fractional equivocation expression from (5.16), the average information leakage rate is written as

$$R_L = \mathbb{E}\{(1 - \Delta)R_S\} = (1 - \bar{\Delta})R_S. \tag{5.20}$$

Remark 7: For higher values of c, the average information leakage rate R_L is dependent on secrecy rate of the system as $R_L \rightarrow R_S/2$. Intuitively, increasing the noise parameter c causes the hitting probability of molecules to decrease. Large c values for the Alice-Eve channel indicate an increase in Eve's distance, thereby decreasing the leakage rate of the system.

Remark 8: For higher secrecy rates the average information leakage rate R_L in (5.20) is dependent on R_S. Clearly, increasing secrecy rate causes the average information leakage rate to increase, thereby leaking more information to Eve.

Remark 9: From a practical perspective, increasing α signifies an increase in the degrada-

tion process of the information molecules. This results in a reduction in the number of molecules that arrive at Eve, decreasing the information leakage rate R_L.

Note that all the aforementioned secrecy metrics give insights into the partial secrecy regime of the system by taking into consideration the decodability of Eve. However, these metrics offer minimal understanding in terms of the confusion level of Eve. Therefore, in the following subsection, we propose a new metric that uses unified second-order statistics to quantify Eve's confusion level severity.

5.3.4 Amount of Confusion Level

In DBMT channels, the effect of Eve for lower values of Lévy noise parameter can not be observed prominently from the GSOP, $\bar{\Delta}$ and the R_L analysis. To overcome these limitations, we propose a newer metric that we call the ACL, which considers the first and the second moments of the fractional equivocation. ACL is the ratio of variance to square of average fractional equivocation. Mathematically, the expression for ACL is given as

$$\text{ACL} = \frac{\mathbb{E}[\Delta^2] - \mathbb{E}[\Delta]^2}{\mathbb{E}[\Delta]^2} = \frac{\mathbb{E}[\Delta^2]}{\mathbb{E}[\Delta]^2} - 1, \tag{5.21}$$

here, $\mathbb{E}[\Delta^2]$ can be written as

$$\mathbb{E}[\Delta^2] = \int_0^{\lambda_1} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm + \int_{\lambda_1}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \left(\frac{(AR_B - 2\ln(m) - B)^2}{(AR_S)^2}\right) dm. \tag{5.22}$$

By using the approximation of $\ln(m) \leq (am^{(\frac{1}{a})} - a)$ from [206, eq.4.1.37] and some algebraic operations the expression of $\mathbb{E}[\Delta^2]$ is written as

$$\begin{aligned}\mathbb{E}[\Delta^2] \approx & 1 - Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) + \left(\frac{(AR_B - B)^2}{(AR_S)^2}\right)\left\{Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2 - \mu_M}{\sigma_M}\right)\right\} \\ & + \left(\frac{(4a^2)((\mu_M)^{\frac{2}{a}} - 2(\mu_M)^{\frac{1}{a}} + 1)}{(AR_S)^2}\right)\left\{Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2 - \mu_M}{\sigma_M}\right)\right\} \\ & - \left(\frac{4a(AR_B - B)((\mu_M)^{\frac{1}{a}} - 1)}{(AR_S)^2}\right)\left\{Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2 - \mu_M}{\sigma_M}\right)\right\}.\end{aligned} \tag{5.23}$$

Proof: The detailed proof is given in Appendix C. Substituting (5.23) and (5.16) in (5.21) the expression for ACL is obtained.

Remark 10: For higher value of c, the expression for second moment ($\mathbb{E}[\Delta^2]$) reduces to $1-Q(\mu_M/\sigma_M)$. Clearly, the second moment is dependent on μ_M and σ_M values. Hence, the expression for ACL reduces to

$$\text{ACL} \approx \frac{1}{1-Q\left(\frac{\mu_M}{\sigma_M}\right)} - 1. \tag{5.24}$$

Remark 11: For large values of secrecy rates (R_S), the amount of confusion level increases. This follows from the fact that at high R_S, the expression $Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right)$ reduces to $Q(\frac{-\mu_M}{\sigma_M})$ which then modifies the second moment as

$$\mathbb{E}[\Delta^2] \approx 1 - Q\left(\mu_M/\sigma_M\right) - Q\left(-\mu_M/\sigma_M\right). \tag{5.25}$$

Based on $\mathbb{E}[\Delta^2]$ and $\bar{\Delta}$ expressions obtained in (5.25) and (5.18) respectively the modified expression for ACL is given as

$$\text{ACL} \approx \frac{1}{1-Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{-\mu_M}{\sigma_M}\right)} - 1 \to \infty. \tag{5.26}$$

Remark 12: Note that for higher α value the expression for second moment $\mathbb{E}[\Delta^2]$ approaches towards $1-Q(\mu_M/\sigma_M)$. Hence, by substituting (5.19) and the modified expression of $\mathbb{E}[\Delta^2]$ into (5.21), the expression for ACL becomes

$$\text{ACL} \approx \frac{1}{1-Q\left(\frac{\mu_M}{\sigma_M}\right)} - 1. \tag{5.27}$$

Therefore, it is clear from the above expression that ACL depends on μ_M and σ_M, which, in turn, depends on the physical parameters α, c, and R_S of the DBMT channel.

Remark 13: It can be noted that $\mathbb{E}[\Delta^2] = \mathbb{E}[\Delta]$, if Δ is a Bernoulli RV. This condition is true when $R_S = 0$ as verified from (5.9). Under this condition, the ACL will be zero, indicating a secure system.

Note that, from (5.21), it can be noted that the ACL metric is analogous to the amount of fading (AoF) in the wireless communication. AoF is a fundamental performance metric used to quantify the severity of fading in wireless environment. Mathematically, the AoF is defined as

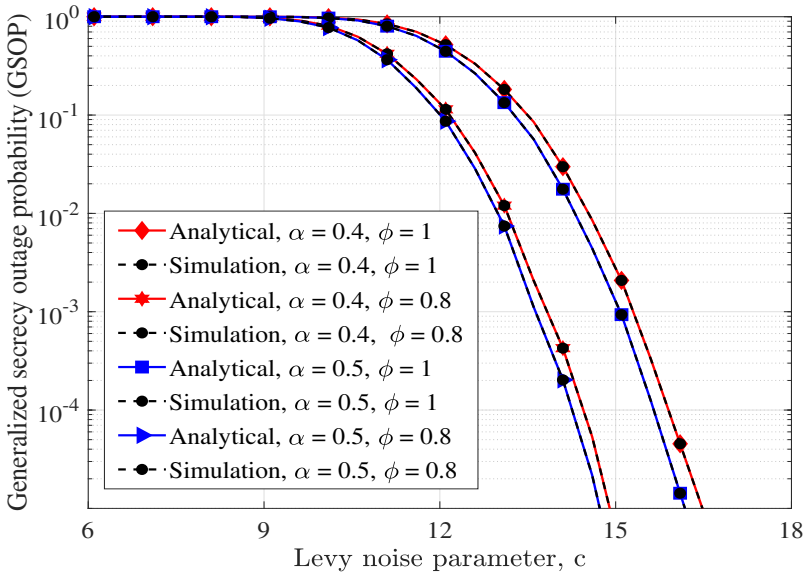

Figure 5.3: GSOP versus c for different values of α and ϕ. The other parameters are $N = 200$, $D = 79.4\ \mu m^2/\text{s}$ [203], $R_S = 0.1$ bits/s, $R_B = 1$ bits/s and $\tau_x = 1$ s.

[207]

$$\text{AoF} = \frac{\text{var}(\gamma)}{(\mathbb{E}[\gamma])^2}, \tag{5.28}$$

where var(.) denotes the variance and γ is instantaneous signal to noise ratio. From (5.28) it is noted that AoF metric is wireless communication system's performance metric which take into account the first and second moments to measure fading severity.

5.4 Numerical Results

In this section, we present numerical results to validate our theoretical analysis and provide insightful discussions. The simulation results have been obtained using particle-based simulations, where all the results are averaged over 50000 independent realizations. All other parameter values are mentioned in the respective figure captions.

The variation of GSOP with c for different α and ϕ values is shown in Figure 5.3. As seen from the plots, with increasing c, the GSOP shows a declining trend. This follows as c increases p_τ decrease, which in turn leads to deterioration in the process of molecule reception by Eve. The decrease in GSOP value creates a positive impact on the secrecy performance of the system, thereby making the system more secure. Note that GSOP also decreases more prominently with a decreasing value of ϕ, and this decline is more pronounced for higher α values. Increasing

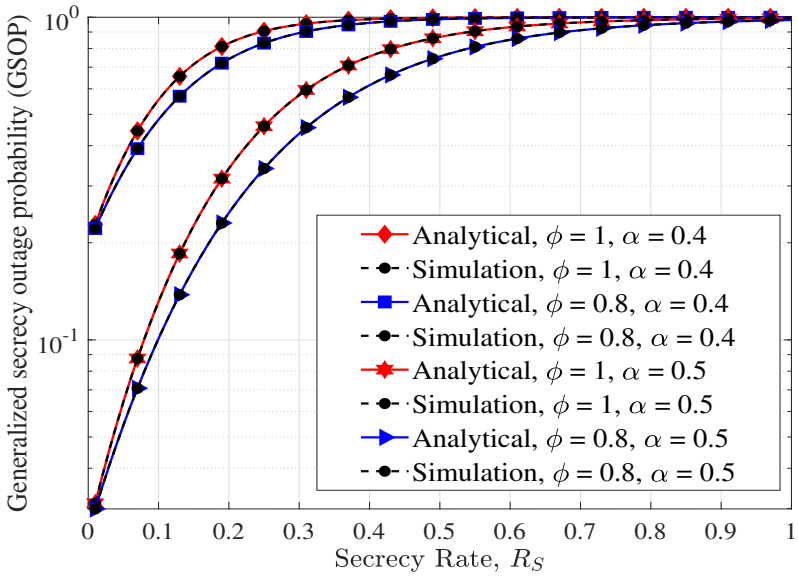

Figure 5.4: GSOP versus R_S for different values of α and ϕ. The other parameters are $N = 200$, $D = 79.4\ \mu\text{m}^2/\text{s}$ [203], $c = 12$, $R_B = 1$ bits/s and $\tau_x = 1$ s.

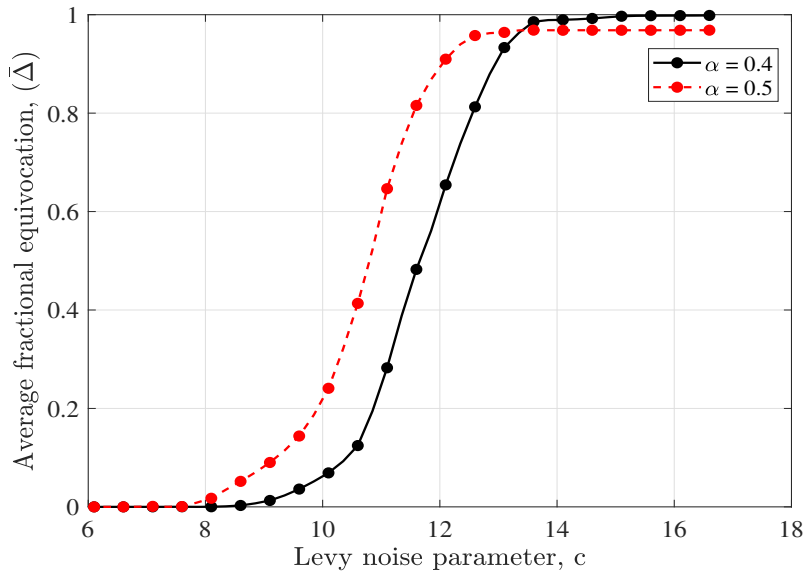

Figure 5.5: Average fractional equivocation versus Lévy noise parameter (c) for different values of α and ϕ. The other parameters are $N = 200$, $D = 79.4\ \mu\text{m}^2/\text{s}$ [203], $R_S = 0.1$ bits/s, $R_B = 1$ bits/s and $\tau_x = 1$ s.

α causes a molecule to disintegrate rapidly, thereby inhibiting the molecule reception process at Eve. Similarly, the GSOP versus R_S variation for different α and ϕ values is illustrated in Figure 5.4. As shown in the figure, with increasing R_S, the system's secrecy deteriorates. These observations confirms our result in (5.12), (5.13), and (5.14).

Figure 5.5 provides the plots between $\bar{\Delta}$ and the Lévy noise parameter c for different values of α. As shown in figure, $\bar{\Delta}$ of the system increases as c increases. This is primarily because for higher c values, p_τ decreases. It can also be noted that the variation of $\bar{\Delta}$ versus c is more prominent at higher values of α. These observations indicate that, increasing c and α has a positive impact on secrecy of system whereas, increasing R_S has a negative impact on the system's secrecy, as observed in (5.17), (5.18), and (5.19).

In Figure 5.6, the effect of c and α on the information leakage rate is considered. As can be seen from the plots, for higher values of c, p_τ decreases, leading to less information leakage towards Eve. Further, it can be noted that for higher α, R_L decreases at a faster rate. This verifies the observation made in **remark** 9.

The effect of c on ACL for different values of α is shown in Figure 5.7. As the plots indicate, the ACL decreases with increasing c. This follows from (5.24) where increasing c decreases p_τ which then decreases ACL. Simultaneously an increasing α accelerates the degradation process, thereby leading to lesser confusion levels at Eve as indicated by (5.27). Similarly, the ACL versus R_S variation for different values of α is illustrated in Figure 5.8. As shown in the figure, with increasing R_S, the ACL increases, whereas for $R_S = 0$ the ACL will be zero. This further verifies the observation made in **remark** 13.

It can be observed from Figure 5.3, Figure 5.4, Figure 5.5 and Figure 5.6 that for c values upto 10, the performance metrics such as GSOP, $\bar{\Delta}$ and R_L cannot clearly illustrate the effect of Eve. Whereas from Figure 5.7, a clear observation regarding the effect of Eve from the ACL metric can be made. Therefore, in less noisy environments the ACL metric is clearly a better metric to analyze the secrecy of DBMT channels.

5.5 Summary

In this chapter we discussed the secrecy analysis of multi-particle diffusive molecular timing channels from the amount of confusion level perspective. Here we calculated various secrecy performance metrics such as GSOP, average fractional equivocation and average information

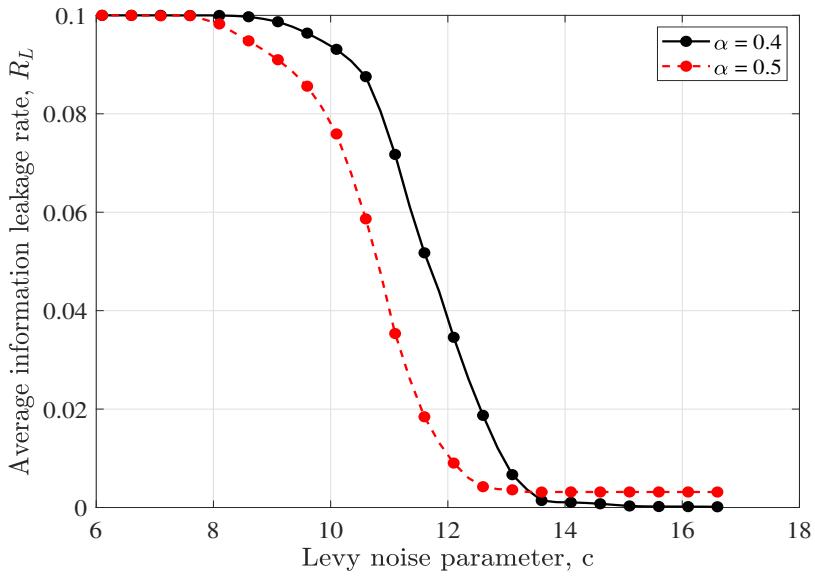

Figure 5.6: Average information leakage rate versus Lévy noise parameter (c) for different values of α. The other parameters are $N = 200$, $D = 79.4\ \mu\text{m}^2/\text{s}$ [203], $R_S = 0.1$ bits/s, $R_B = 1$ bits/s and $\tau_x = 1$ s.

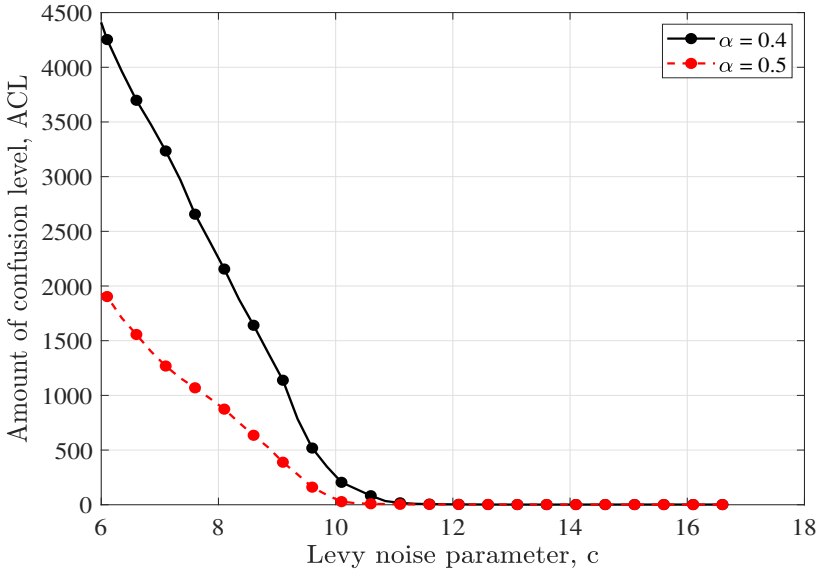

Figure 5.7: Amount of confusion level versus Lévy noise parameter (c) for different values of α. The other parameters are $N = 200$, $D = 79.4\ \mu\text{m}^2/\text{s}$ [203], $R_S = 0.1$ bits/s, $R_B = 1$ bits/s and $\tau_x = 1$ s.

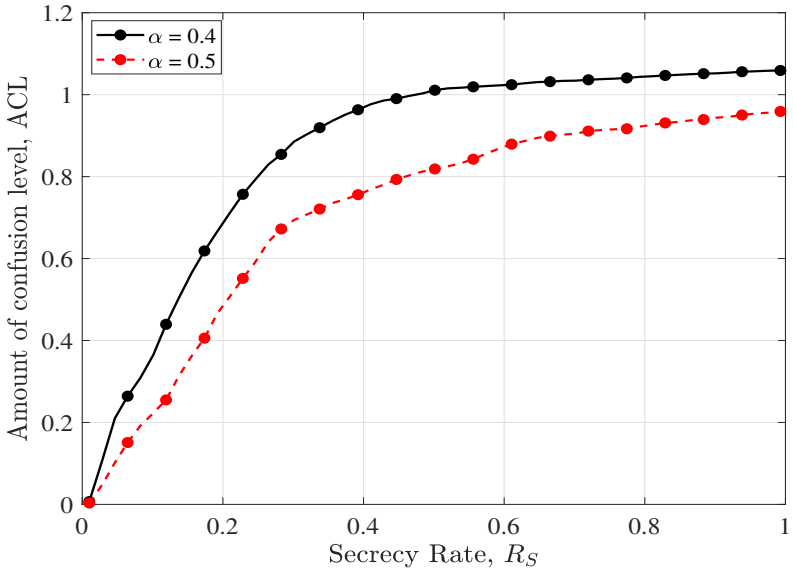

Figure 5.8: Amount of confusion level versus R_S for different values of α. The other parameters are $N = 200$, $D = 79.4\ \mu\text{m}^2/\text{sec}$ [203], $c = 12$, $R_B = 1$ bits/s and $\tau_x = 1$ s.

leakage rate from the partial secrecy perspective. Using the average fractional equivocation expression we then defined the secrecy based on the second order statistics of the system. The second order statistics especially in terms of amount of confusion level gives a more useful insights on the secrecy aspects of diffusive molecular timing channels.

Chapter 6

Secrecy Loss in DBMT channels

6.1 Introduction

In this chapter, a new secrecy performance metric of the DBMT channel is discussed. Here, we present the amount of secrecy loss (ASL) of the DBMT channel in the presence of an Eve. ASL is a useful second-order metric for quantifying the severity of confidential information leaked towards Eve. Similar to the amount of confusion level metric discussed in the previous chapter, the ASL metric is analogous to the amount of fading metric used in a wireless scenario. The second-order metric is usually helpful in gaining insights into the system's dynamics, which would subsequently help in analyzing the system's secrecy performance in terms of various secrecy performance metrics. In this chapter, we first derive the secrecy outage probability (SOP) expression and using the SOP expression, we then calculate the system's average secrecy rate (ASR) when the number of molecules at Eve follow Gaussian distribution. Finally, we then derive the ASL expression of the system model under consideration using the ASR expression.

6.2 System Model

In this chapter the secrecy loss in DBMT channels is discussed. For this a 1-D environment where an authorized transmitter, Alice is located between a legitimate receiver, Bob and an eavesdropper, Eve is considered. Alice wants to transmit information to Bob over a DBMT channel, where information to be transmitted is encoded in the time of release. Figure 6.1 represents the eavesdropping scenario in DBMT channel. Alice is considered to be a point source that can release an impulse of N identical molecules in the aqueous media. Meanwhile,

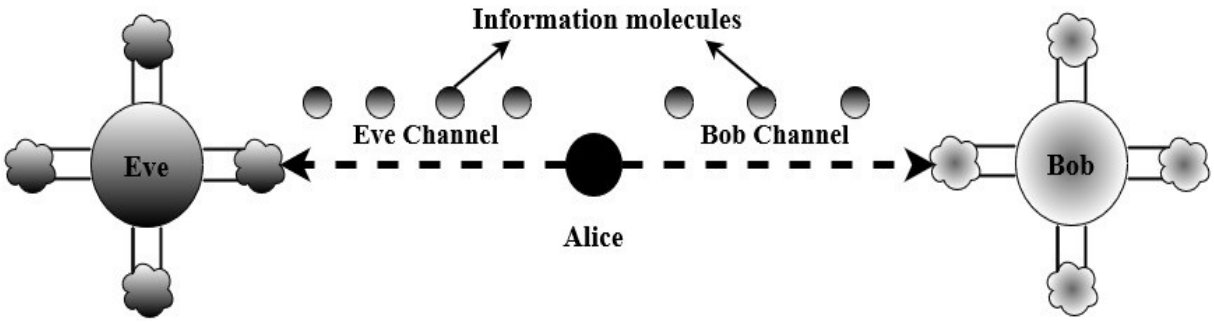

Figure 6.1: Scenario of eavesdropping in diffusion-based molecular timing channels [203].

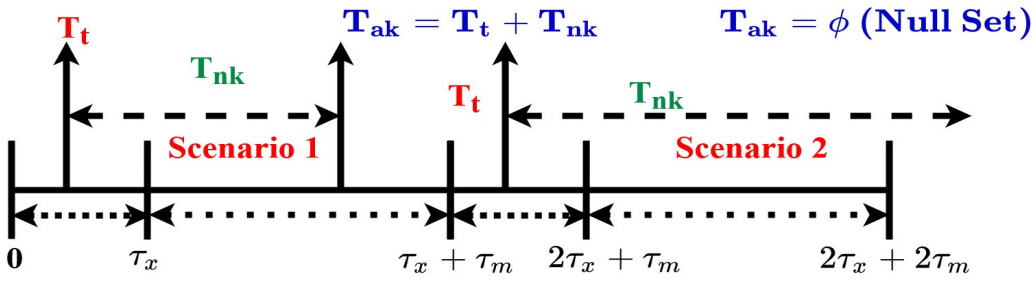

Figure 6.2: Timing model of DBMT channels [165].

both Bob and Eve are assumed to be fully absorbing receivers. The media is free from the drift phenomenon, and each transmitted molecule follows an independent path with a finite lifetime. Since the information is in the time of release, so for each particle, the transmission time is denoted as T_t. Each particle then follows a random independent propagation path and arrives at a particular time of arrival represented as T_a. This arrival time is sum of T_t and random propagation delay T_n. Mathematically, representation is given as

$$T_{a_k} = T_t + T_{n_k} \quad \text{for} \quad T_{n_B}, T_{n_E} \leq \tau_m, \tag{6.1}$$

where $k \in \{\text{Bob}(B), \text{Eve}(E)\}$ and $\tau_m = \frac{1}{\alpha}\ln\left(\frac{100}{X}\right)$ be the time taken by the information molecule to decay to $X\%$ of its initial value with α being the degradation parameter [82]. After $X\%$ of degradation, the molecules are rendered useless and are removed from the media in order to avoid ISI in the system. Figure. 6.2 represents the timing model of a DBMT channel. As observed from the figure there are two scenarios in any DBMT channel. Scenario 1 corresponds to a case when $T_{n_k} \leq \tau_m$, in which molecular reception at Bob and Eve is ensured with information in T_{a_k}. However, scenario 2 corresponds to a case where $T_{n_k} > \tau_m$ in which molecules does not arrive at Bob or Eve. Therefore in scenario 2, no information goes through the channel and T_{a_k} corresponds to a null set (ϕ). Moreover, from (3.4) and figure, the T_{n_k} of the system behaves as an additive noise term and for a drift free scenario this additive noise term can be

modeled as α-stable Lévy distributed RV (Lévy(μ_k, c_k)) [81]. Mathematically, probability density function (p.d.f) of Lévy distributed RV can be represented as [82, eq. (4)] where μ is the location parameter and c is the Lévy noise parameter expressed as $c_k = \frac{d_k^2}{2D}$ where d_k is the distance travelled by the molecule and D is the diffusion coefficient. In general, T_{n_k} can be written as $T_{n_k} \sim$Lévy$(0, d_k^2/(2D))$ with p.d.f denoted as $f_{T_{n_k}}(t_{n_k}) = \sqrt{\frac{c_k}{2\pi t_n^3}} \exp\left(-\frac{c_k}{2t_n}\right)$[82, eq. (7)]. The stability of the Lévy distributed RV usually results in the non existence of finite moments, making it difficult to characterize and analyze the drift-free diffusive molecular communication channels. So, we employ an exponential degradation model to characterize the lifetime of information molecules which mathematically is expressed as

$$h(\tau_n) = \alpha e^{-\alpha \tau_n}, \qquad \tau_n > 0, \tag{6.2}$$

where τ_n represents the *lifetime of the information* molecules and $h(\tau_n)$ is the exponentially decaying lifetime rate. Note that τ_m corresponds to time required by molecules to decay to a state beyond which receiver would not be able to recognize, where τ_m can be expressed as $\tau_m \leq \tau_n$. Therefore, using $h(\tau_n)$ and $f_{T_n}(t_n)$, the random propagation delay T_{n_k} of the information molecules in a drift free environment can be modelled as truncated Lévy distribution which mathematically is represented as

$$f_{t_d} = k' \sqrt{\frac{d^2}{4\pi D t_d^3}} \mathrm{e}^{-\frac{d^2}{4Dt_d}} \mathrm{e}^{-\alpha t_d} \quad \text{for} \quad t_d > 0, \tag{6.3}$$

where k'=exp(p) is the normalizing factor and p is the scaled version of the noise parameter given by p=$\sqrt{2\alpha c}$. Note that the exponential degradation modelling helps in creating an inter-symbol interference (ISI) free channel. Taking an approach similar to [82], let $\tau_m = \frac{1}{\alpha}\ln\left(\frac{100}{X}\right)$ be the time taken by the information molecule to decay to $X\%$ of its initial value. After $X\%$ of degradation, the molecules are rendered useless and are removed from the media in order to avoid ISI in the system. Note that the exponential degradation rate and finite lifetime of the molecules gives us a provision to create *sufficient large duration* time slots which not only overcome ISI but also prevent the out of order arrival of the molecules at Bob or Eve. Similar to [82], in our case also each time slot τ_s satisfies $\tau_s = \tau_x + \tau_m$, where τ_x represents the symbol interval in which the molecules are transmitted. The number of identical particles transmitted by Alice at a particular instant T_t is represented by N. The number of molecules released by Alice is also same for all the input messages. Note that the simultaneous release of multiple

particles corresponds to receiver diversity and the simultaneous release of N particles increases the capacity of the DBMT channel. Let M_k denoted the number of information molecules that arrive at Bob or Eve within a time slot. Note that the number of information molecules released by Alice is large enough such that $M_k \geq N_c$, where N_c is the cross-over point between Lévy and Gaussian regimes. N_c can be obtained by expression as obtained in [82, eq.(25)]. Since the path followed by the information molecules is independent and identically distributed therefore according to central limit theorem the number of molecules reaching Eve can be taken to be Gaussian distributed. Based on this, let M_E be Gaussian distributed RV represented as $\mathcal{N}(\mu_M, \sigma_M^2)$ where $\mu_M = Np_{\tau_E}$ is mean and $\sigma_M^2 = Np_{\tau_E}(1-p_{\tau_E})$ is the variance. Let p_{τ_k} denote the individual hitting probability of the molecule within a time interval and given by [82, eq.(32)]

$$p_{\tau_k} = k' \sqrt{\frac{c_k}{2\pi}} \left(2\sqrt{\frac{p_k}{c_k}} K_{1/2}(p_k) - \sqrt{\frac{1}{\tau_m}} K_{1/2}\left(\alpha\tau_m, \frac{c_k}{2\tau_m} \right) \right), \tag{6.4}$$

where p_k is the scaled version of the noise parameter given by $p_k{=}\sqrt{2\alpha c_k}$, $K_v(x)$ and $K_v(x,y)$ are the modified Bessel's function of second kind and incomplete Bessel's function. Using this formulation, for large N the existing upper bound on the capacity is given by [82, eq.(55)], which can be further simplified as

$$C_k = \max_{\tau_x} \frac{2\ln(M_k) + F}{A}, \tag{6.5}$$

where $A = 2\ln(2)(\tau_s)$ and $F = 2\ln(\tau_s) - \ln(2\pi e/\alpha^2)$. Subsequently, C_B and C_E represents the channel capacities of Bob and Eve channels respectively, while M_B and M_E are molecules received at Bob and Eve respectively. The presence of Bob and Eve simultaneously in the DBMT environment contribute towards mutual dependence in terms of molecular reception. It is found that mutual dependence between Bob and Eve is due to α. In any practical MC system d_B can be calculated according to [188]. For a given transmission rate ($R_B \leq C_B$) and d_B values, we calculate α of the system using (6.5). This value of α is used to analyze the secrecy of the system showing the mutual impact.

6.3 Secrecy Performance Metrics

The major focus of this section, is on calculating system model's secrecy in terms of secrecy outage probability (SOP), average secrecy rate (ASR) and amount of secrecy loss (ASL) analysis when the number of particles at Eve follows the Gaussian regime.

6.3.1 Secrecy Outage Probability (SOP)

Generally, the instantaneous secrecy rate is given as

$$R_S = \max(C_B - C_E, 0). \tag{6.6}$$

In the case where the instantaneous channel state information (CSI) of the Eve channel is not known at Alice, this corresponds to the passive eavesdropping regime. Therefore, under this, the system's secrecy performance is measured by secrecy outage probability (SOP). This secrecy performance metric gives insights into how information integrity is maintained when Eve's instantaneous CSI is not known at Alice. In such scenarios, Alice transmits information securely with a certain rate R_λ. Mathematically, SOP expression for passive eavesdropping is given as

$$P_{out} = \mathbb{P}(R_S \leq R_\lambda) = \mathbb{P}\left(M_E \geq \mathrm{e}^{\frac{AR_B - AR_\lambda - F}{2}}\right) = \int_{\lambda_1}^{\infty} \frac{\mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}}{\sqrt{2\pi\sigma_M^2}}\, dm \;=\; Q\left(\frac{\lambda_1 - \mu_M}{\sqrt{\sigma_M^2}}\right), \tag{6.7}$$

where $\lambda_1 = \mathrm{e}^{\frac{AR_B - AR_\lambda - F}{2}}$, R_B is the Bob's transmission rate and $Q(.)$ is the Q-function.

Remark 1: To obtain more insights, we develop asymptotic SOP analysis for the DBMT channel. Following are the observations made:

- SOP is directly proportional to λ_1 which in turn is dependent exponentially on R_B. Let $R_B \to \infty$, while α and σ_M^2 are unchanged, corresponds to a case where Bob is very close to Alice with $p_{\tau_B} \to 1$. This observation demonstrate that the quality of Bob channel is better than Eve channel and from (6.7) we found that $P_{out} \to 0$ indicating secrecy improvement.

- For given R_B and σ_M^2, P_{out} depends directly on λ_1 which consecutively is a function of α. Therefore increasing α leads to decrease in λ_1 which implies $P_{out} \to 1$ and results to degrades secrecy. Increasing α practically corresponds to smaller molecular lifetime and

an increase in channel reusability therefore leading to an increase in Eve's capacity (C_E). Increase in C_E leads to deterioration in terms of secrecy.

- P_{out} is inversely proportional to σ_M^2 for the given value of α and R_B. Therefore, from (6.7) $\sigma_M^2 \to \infty$, leads to $P_{out} \to 0.5$.

6.3.2 Average Secrecy Rate (ASR)

Now for the scenario when the CSI of Eve is known at Alice, which is an active eavesdropping scenario, the ASR metric is usually employed as a secrecy performance metric to analyze the secrecy of the system. For calculating ASR, usually, the distributions about M_B and M_E are taken into consideration. However, in the undertaken analysis, an alternate method is employed to calculate the ASR. Since in ASR the secrecy rate is a random quantity with certain statistical properties, thus it becomes imperative to obtain the CDF expression $F_{R_S}(y)$ by replacing R_S with y in the SOP expression. Therefore, mathematically ASR can be represented as

$$ASR = \int_0^\infty (1 - F_{R_S}(y))\, dy = \int_0^\infty \left(1 - Q\left(\frac{\mathrm{e}^{\frac{A(R_B-y)-F}{2}} - \mu_M}{\sqrt{\sigma_M^2}}\right)\right) dy. \tag{6.8}$$

Now by using $Q(.)$ function approximation as given by [202, eq.(8)] and substituting $\mathrm{e}^{\frac{A(R_B-y)-F}{2}} - \mu_M = t$ the ASR expression can be modified to

$$ASR \approx \frac{2}{A}\int_{t_2}^{t_1} \left(1 - \frac{\mathrm{e}^{-\frac{t^2}{2\sigma_M^2}}}{12} - \frac{\mathrm{e}^{-\frac{2t^2}{3\sigma_M^2}}}{4}\right) \frac{dt}{\mu_M + t}. \tag{6.9}$$

Thus the closed-form expression for ASR is obtained as

$$\begin{aligned} ASR \approx \frac{2}{A\mu_M}\Bigg(t_1 - t_2 - \frac{\sqrt{2\pi\sigma_M^2}}{24}\left(\mathrm{erf}\left(\frac{t_1}{\sqrt{2\sigma_M^2}}\right) - \mathrm{erf}\left(\frac{t_2}{\sqrt{2\sigma_M^2}}\right)\right) \\ - \frac{\sqrt{6\pi\sigma_M^2}}{16}\left(\mathrm{erf}\left(\sqrt{\frac{2}{3\sigma_M^2}}t_1\right) - \mathrm{erf}\left(\sqrt{\frac{2}{3\sigma_M^2}}t_2\right)\right)\Bigg), \end{aligned} \tag{6.10}$$

where $t_1 = \mathrm{e}^{\frac{AR_B-F}{2}} - \mu_M$, $t_2 = -\mu_M$ and erf(.) is the error-function.

Remark 2: Following are the observations made from the asymptotic ASR analysis.

- It is found that ASR is directly proportional to t_1 using (6.10). Further, t_1 is increasing function of R_B. For given α and σ_M^2, p_{τ_B} will improve with R_B resulting into improvement in Bob's channel. Asymptotically as $R_B \to \infty$, $t_1 \to \infty$ indicating ASR$\to \infty$. Therefore, R_B has a positive impact on system's ASR.

- For a given R_B and σ_M^2, $p_{\tau_B} \to 0$ as $\alpha \to \infty$ indicating $t_1 \to -\mu_M$. Further it can be concluded using (6.10) that ASR$\to 0$ and hence the secrecy of the system degrades.

- From (6.10) σ_M^2 has a negative impact on the ASR of the system. Increasing σ_M^2 deteriorates ASR and hence leads to compromising in terms of secrecy.

Note that the SOP and the ASR metrics according to (6.7) and (6.10) respectively are used to quantify the secrecy of the system from the perspective of first order statistics. However, the first order statistics contains certain practical limitations as first-order statistics does not give any information regarding the amount at which the confidential information is leaked to Eve. Therefore from practical point of view in the next subsection we use ASL metric to characterize and analyze the severity of information loss in DBMT channels.

6.3.3 Amount of Secrecy Loss (ASL)

The amount of secrecy loss (ASL) is a different secrecy performance metric which gives the information about the severity of confidential information leaked from Alice to Eve. ASL is related to R_S according to the expression given by

$$ASL = \frac{E[R_S^2]}{E[R_S]^2} - 1, \tag{6.11}$$

where $E[.]$ denotes the expectation operator and $E[R_S]$=ASR. Basically, ASL is nothing but the ratio of variance and square of mean. To calculate ASL one first need to calculate $E[R_S^2]$ which mathematically written as

$$E[R_S^2] = 2\int_0^\infty y(1 - F_{R_S}(y))dy. \tag{6.12}$$

By substituting (6.7) in (6.12) and using the approximate expression of $Q(.)$ function the above expression of $E[R_S^2]$ can be modified as

$$E[R_S^2] \approx \frac{8}{A^2}\int_{t_2}^{t_1} \frac{\ln\left(\frac{\lambda}{t+\mu_M}\right)}{\mu_M + t}\left(1 - \frac{e^{-\frac{t^2}{2\sigma_M^2}}}{12} - \frac{e^{-\frac{2t^2}{3\sigma_M^2}}}{4}\right)dt, \tag{6.13}$$

where $\lambda = e^{\frac{AR_B - F}{2}}$. Therefore, by using integral properties and after some algebraic operations the closed form expression of the integral in (6.13) is given as

$$E[R_S^2] \approx \frac{8\lambda}{A^2\mu_M} - \ln\left(\frac{\lambda}{\mu_M}\right)\left\{\frac{8\sqrt{2\pi\sigma_M^2}}{24A^2\mu_M}\left\{\text{erf}\left(\frac{t_1}{\sqrt{2\sigma_M^2}}\right) + \text{erf}\left(\frac{t_2}{\sqrt{2\sigma_M^2}}\right)\right\}\right.$$
$$\left. + \frac{8\sqrt{6\pi\sigma_M^2}}{16A^2\mu_M}\left\{\text{erf}\left(\sqrt{\frac{2}{3\sigma_M^2}}t_1\right) + \text{erf}\left(\sqrt{\frac{2}{3\sigma_M^2}}t_2\right)\right\}\right\}. \quad (6.14)$$

Substituting (6.10) and (6.14) in (6.11) the expression for ASL can be obtained.

Remark 3: Based on above analysis following highlights some observations regarding ASL of the system

- R_B has a positive impact on system's secrecy as for higher R_B values, the ASR of the system increases and subsequently from (6.11) the ASL value decreases. Particularly as $R_B \to \infty$, the ASR$\to \infty$ and thus from (6.11) ASL$\to 0$ which shows that the system operates in the safe region with no unnecessary interruptions.

- As $\alpha \to \infty$, ASR$\to 0$ as discussed in remark 2, therefore according to (6.11) the ASL$\to \infty$.

- Using remark 2, increasing σ_M^2 leads to decrease in ASR of the system with ASR$\approx$0 when $\sigma_M^2 \to \infty$. For such systems ASL$\to \infty$ according to (6.11). This means that Eve can decode full information leading to secrecy compromisation and regular system interruptions.

ASL is a second-order metric implemented to calculate the severity of information leaked to Eve. From (6.11), it can be noted that the ASL being a second-order metric utilizes higher order moments to parameterize the severity of information leaked to Eve. ASL metric can always be used where there is a trade-off between various secrecy metrics in terms of system parameters, thereby increasing the DBMT channel's secrecy performance.

Remark 4: The analysis presented in the chapter is concentrated on 1-D channel model implemented in chemical synapse and bio-chips environments where length dimension is substantial compared to other dimensions. However, as stated in [165], the first arrival time in an infinite, 3-D homogeneous medium without flow containing absorbing receivers, follows a scaled Lévy distribution. Therefore, the results presented in the chapter can be extended to 3-D by introducing a scalar multiple.

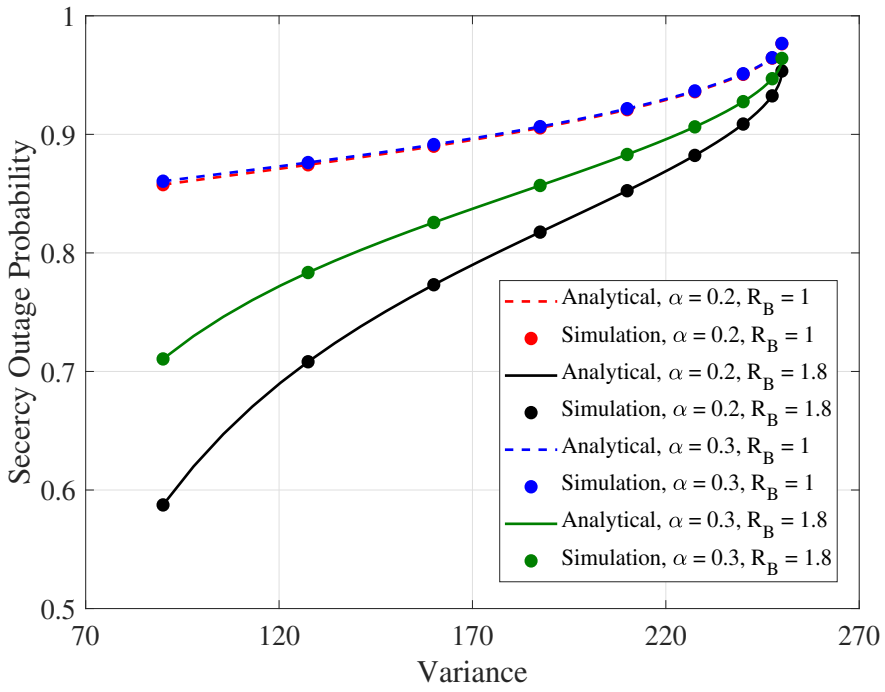

Figure 6.3: Secrecy outage probability versus variance for different values of α and R_B. The other parameters are $N = 1000$, $R_\lambda = 1$ bits/s and $D = 79.4\mu\text{m}^2/\text{s}$ [6].

6.4 Numerical Results

Based on the mathematical analysis presented in the previous section, in this section, the numerical results for the proposed system model to validate SOP, ASR and ASL's effect in multi-particle DBMT channels is undertaken. Here the plots pertaining to the secrecy performance in terms of SOP, ASR and ASL metrics for the various value of α and R_B is analyzed. The simulation results have been obtained using particle-based simulations, where all the results are averaged over 70000 independent realizations. All other parameter values are mentioned in the respective figure captions. The variation of SOP as a function of Eve variance for different values of α and R_B is shown in Figure 6.3. As seen from the plot, the SOP of the system increases with increasing σ_M^2. This follows as σ_M^2 increases the molecular reception increases. It can be further noted that SOP decreases as both α and R_B increases; however, the decrease in SOP is more prominent when R_B increases.

Figure 6.4 represents the plot between ASR and the variance for different values of α as well as for different R_B. From the figure, it is evident that with increasing variance, the ASR of the system decreases. This is because increasing variance leads to more reception of molecules by Eve as compared to Bob. Thus increasing variance has a negative impact on ASR. Further, in-

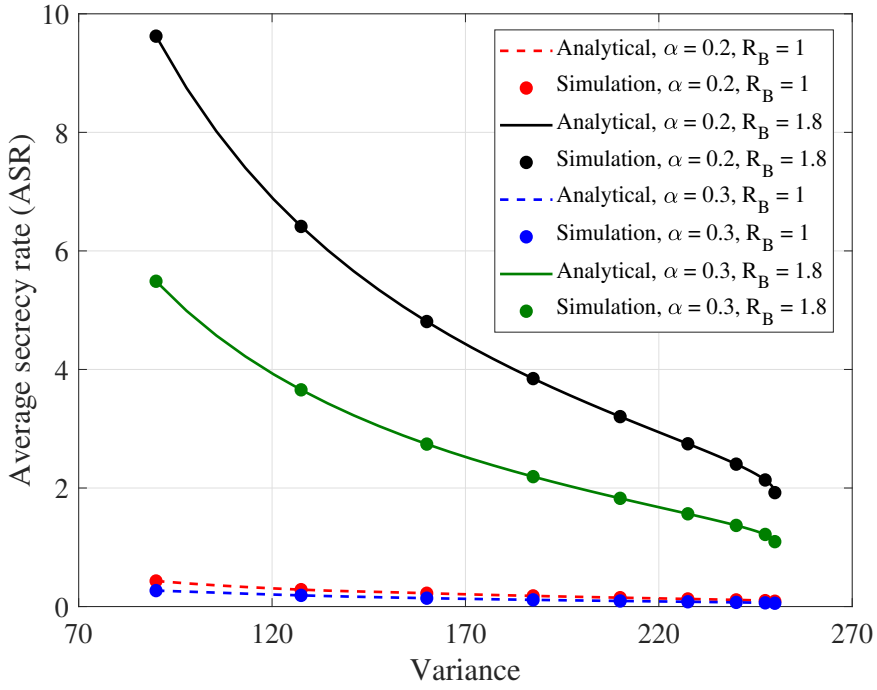

Figure 6.4: Average secrecy rate versus variance for different values of α and R_B. The other parameters are $N = 1000$ and $D = 79.4\ \mu\text{m}^2/\text{s}$ [6].

creasing α causes the molecule to degrade rapidly, thereby decreasing the multi-particle DBMT channel's secrecy rate. Additionally, by increasing R_B, the secrecy performance, especially the ASR of the system, improves.

Figure 6.5 shows the plot between ASL as a function of variance for different values of α and R_B. From the figure, it can be observed that with increasing variance, the ASL shows an increasing trend. As the variance is increased, the ASR decreases, and this decreasing ASR, in turn, increases the ASL of the system, thereby degrading the system's secrecy performance. Moreover, for increasing α, the ASL plot shows an increasing trend. This is because for increasing α, the ASR decreases, which in turn increases ASL. Simultaneously, for increasing R_B, the amount of secrecy loss is less, thereby preventing secrecy loss in the system.

It can be observed from Figure 6.3 and Figure 6.4 that for higher variance neither SOP metric nor ASR metric provide a clear effect of Eve. However, the ASL metric, as shown in Figure 6.5 clearly show the effect of Eve even at high variances. Thus, for highly noisy environments, the ASL metric compared to its existing metrics is a better alternative to quantify Eve's effect in DBMT channels. Moreover, in practical MC systems, the SOP and ASR metrics being first-order metrics do not provide the designer flexibility from a secrecy perspective. Therefore, it is recommended to use the ASL metric as a design-oriented metric to analyze DBMT channel's

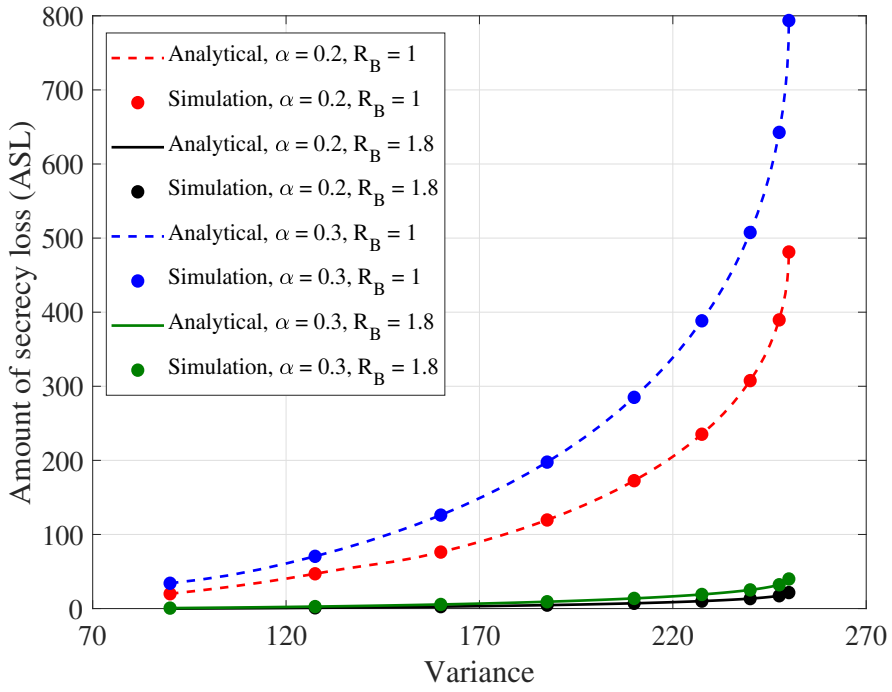

Figure 6.5: Amount of secrecy loss versus variance for different values of α and R_B. The other parameters are $N = 1000$ and $D = 79.4\ \mu\text{m}^2/\text{s}$ [6].

secrecy performance.

6.5 Summary

In this chapter, we analyzed the amount of secrecy loss in DBMT channels when the number of particles received at Eve is assumed to follow Gaussian distribution. Here, first we calculated the secrecy outage probability of the timing channel. Subsequently, we calculated the average secrecy rate of the diffusive molecular timing channels. Finally, we calculated the amount of secrecy loss by using the expressions of SOP and ASR. The ASL analysis provide useful insights, especially in terms of the severity of secure information loss towards Eve and its implication and its implications in the DBMT channels. The analysis undertaken in this chapter will help to bridge the gap between the theoretical and practical aspects of secrecy performance in multi-particle DBMT channels.

Chapter 7

Conclusion

Molecular communication (MC) is an emerging bio-inspired field where the exchange of information between various nano-machines is accomplished via chemical exchange. This chemical exchange of information molecules enables systematic transmission, propagation, and reception of information between transmitter and receiver. Inspired by nature, MC can act as a promising means of communication between nano-devices in numerous practical applications. Since MC finds its prominent applications in biomedical and healthcare scenarios, where information is private sensitive, securing user's information comes into the picture. Being a new domain in MC, not much work has been reported in the literature. Therefore, it becomes imperative that the problems related to secrecy in the MC paradigm are addressed at the start rather than adding secrecy to the MC systems later.

The focus of this Ph.D. thesis is to address the secrecy concern in the diffusion-based molecular timing (DBMT) channels where information is in the time of release of molecules. In the thesis, we have employed free diffusion for the propagation of information particles. Further, the information molecules follow a random path and the random propagation delay is modelled as truncated Lévy distribution. The information molecules transmitted by the transmitter are identical; therefore, the concept of secrecy in MC based systems becomes a significant issue. Moreover, because of the dearth of research in secrecy aspects of the MC, an eavesdropper's effect on MC-based systems becomes challenging. Therefore, the research undertaken in the thesis provides a fundamental framework to implement secrecy in DBMT channels by analyzing the effect of an eavesdropper in the DBMT channels.

The objectives of the research presented in the thesis are to analyze the secrecy performance of DBMT channels by employing various secrecy performance metrics. For this, we

first calculated the upper bound on the average eavesdropper capacity of single-particle DBMT channels when the distance of the eavesdropper is uniform and Gaussian distributed. Second, we analyzed the secrecy performance of single-particle DBMT channels in the partial secrecy regime using various secrecy performance metrics such as generalized secrecy outage probability (GSOP), average fractional equivocation and average information leakage rate. Third, we optimized various secrecy performance metrics and calculated various optimal transmission rates, which would minimize GSOP, maximize average fractional equivocation, and minimize average information leakage rate. Fourth, we examined the secrecy from a confusion level perspective by calculating the amount of confusion level expression. Fifth, we explored the system's secrecy from the secrecy loss perspective, where we calculated the amount of secrecy loss in multi-particle DBMT channels. The analytical results presented in the thesis were also validated by undertaking particle-based simulations. This work would further help to bridge the gap between theoretical and practical aspects in MC based systems.

7.1 Contributions

The main contributions included in each chapter of the thesis are summarized in the following. In chapter 3, we studied the secrecy performance of single-particle DBMT channels. In particular, the main contributions of chapter 3 are as follows:

- We obtained the closed-form expressions of the upper bound of the average capacity of the eavesdropper channel when the distance between transmitter and eavesdropper is assumed to be uniform and Gaussian distributed.
- We provided analytical expression for generalized secrecy outage probability 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 were further drawn from the expression of generalized secrecy outage probability.
- We calculated closed-form expression for average fractional equivocation of the system when the distance between transmitter and eavesdropper is assumed to be uniform and Gaussian distributed. The average fractional equivocation analysis indicates the decoding error probability of an eavesdropper.

- We analyzed the secrecy of the system from the average information leakage rate perspective. For this, we derived the expression for the average information leakage rate to the eavesdropper 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.

Based on the analysis, we learnt that generalized secrecy outage probability shows a decreasing trend when the eavesdropper variance increases, wherein the decrease is more prominent with increasing values of degradation parameter. Similarly, the average fractional equivocation decreases with increasing variance. Moreover, the information leakage rate characterizes the amount of information leaked when the scenario of classical secrecy is not obtained.

Subsequently, in chapter 4, we optimized various secrecy performance metrics of single-particle DBMT channels. In particular, the contributions are:

- We first obtained an approximate expression for the upper bound on the channel capacity. Based on this approximate expression, we calculated the transmission probability when eavesdropper distance is uniform distributed, which is then used for calculating maximum achievable throughput.

- Using the throughput analysis, we calculated the optimal secrecy rate and optimal transmission rate of Bob. Based on the optimal design parameters values, we minimize GSOP, maximize average fractional equivocation and minimize the average information leakage rate, respectively.

Based on the optimization analysis, we found optimal secrecy and Bob's optimal transmission rates, which would be useful for minimizing GSOP, maximizing average fractional equivocation, and minimizing average information leakage rate, respectively. From the numerical results, it can be observed that there is always a trade-off between different optimal design parameters that minimize the generalized secrecy outage probability and maximize the average fractional equivocation and minimize the average information leakage rate.

Chapter 5 highlighted the secrecy analysis of multi-particle DBMT channels from the amount of confusion level perspective. Particularly, the main contributions are:

- We analyzed various secrecy performance metrics for multi-particle DBMT channels. From the numerical results, we learn that compared to secrecy analysis done in the single-particle scenario, the multi-particle secrecy scenario provides more practical insights.

For this, we considered the case where the number of molecules received by Eve was considered to be Gaussian distributed.

- We proposed a new secrecy metric in terms of the amount of confusion level (ACL) of Eve and derived its closed-form expression. Compared to the existing secrecy metrics, this new secrecy metric provides a more robust and distinct secrecy analysis in the multi-particle scenario.

- We showed that any change in the physical parameters such as the Lévy noise parameter and the degradation rate, the secrecy performance of the system gets affected significantly. Especially, increasing the noise parameter leads to an improvement in the secrecy performance of the system.

Through the analytical results presented in the chapter, we observed that the ACL metric characterizes Eve's effect on the DBMT channels in a better way. Moreover, we also showed via numerical results that compared to existing secrecy performance metrics such as GSOP, $\bar{\Delta}$, and R_L, the proposed ACL metric can be used as an alternative metric to analyze the secrecy in multi-particle DBMT channels. Further, through the remarks, we observed that with an increase in Lévy noise parameter, the GSOP, R_L and ACL of the system decreases, while $\bar{\Delta}$ increases, which in turn improves the secrecy of the system.

Finally, in chapter 6, we majorly focused our analysis on the amount of secrecy loss in DBMT channels. The main contributions are:

- We obtained the SOP expression using the existing expression of the capacity upper bound when the molecules received at Eve were assumed to be Gaussian distributed. Based on the SOP expression, we then calculated the ASR expression. The ASR and SOP expressions were used to calculate the closed-form expression for the ASL metric in the multi-particle scenario.

- We identified that the SOP metric based on first-order statistics does not provide any practical information concerning the amount of information loss towards Eve. Therefore, the ASL metric can be used to provide insights into the dynamics of the system's secrecy performance, especially in terms of the amount of information loss towards Eve.

Based on the secrecy loss analysis, we found that using second-order metrics to quantify the secrecy in a multi-particle scenario leads to a more robust secrecy analysis. The ASL metric is

an important second-order metric that can quantify the severity of information loss in the MC environment compared to the classical SOP analysis.

7.2 Scope for future research

In the future, we plan to extend our research, especially in terms of secrecy performance of the MC system, by including 1) a multi-dimensional scenario, especially in a 3-D diffusive environment where the mutual influence in terms of molecular reception at Bob and Eve on each other is very prominent; 2) the study of secrecy in other channel models incorporating different propagation mechanism, e.g., drift scenario with AIGN channels, and molecular motors; 3) the study of a more practical secrecy environments where the effect of the interferer is also prominent; 4) the analysis of the DBMT channels by incorporating the effect of ISI can also be an important study for future; 5) exact expressions for secrecy capacity, SOP, GSOP etc.; 6) the calculation of optimal value for τ_x which provides an optimal input distribution used for calculating the achievable capacity of the DBMT channels; 7) the MC systems finds similarity with the optical communication systems, where photons are employed as information-carriers, so a comparative analysis can be done; 8) the MC systems can also be employed as a means of communication between the nano-robots.

Appendix A

Approximate Upper Bound Capacity

Recall that the capacity upper bound according to [80] is given by:

$$\begin{aligned} C_{ub} \leq & \ln(\mathrm{e}) + \ln\left(\left(\tau_s + \frac{c}{p}e^{-p}\right)e\right) + \frac{3}{2}\sqrt{\frac{p}{2\pi}}I_{1/2}(p)\ln\left(\frac{p}{c}\right) \\ & - \frac{e^{-p}}{2} - \left(\frac{2p\,e^{-p}}{2}\right) + \left(\frac{e^{-p}}{2}\right)\ln\left(\frac{c}{2\pi}\right) + \frac{e^{p}Ei(-2p)}{2\pi} - \frac{e^{-p}Ei(2p)}{2\pi}. \end{aligned} \tag{A.1}$$

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:

$$\begin{aligned} C_{ub} \approx & \ln(\mathrm{e}) + \ln\left(\tau_s + \frac{c}{p}e^{-p}\right) - \frac{e^{-p}}{2} - \left(\frac{2p\,e^{-p}}{2}\right) \\ & + \left(\frac{e^{-p}}{2}\right)\ln\left(\frac{c}{2\pi}\right) + \frac{e^{p}Ei(-2p)}{2\pi} - \frac{e^{-p}Ei(2p)}{2\pi} \end{aligned} \tag{A.2}$$

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

$$C_{ub} \approx 1 + d\sqrt{\frac{\alpha}{D}} + \ln(\tau_s) \tag{A.3}$$

Now by substituting the expression of τ_s from (3.8) and putting $\tau_x = 1$ we have,

$$\ln(\tau_s) \approx \ln\left(\tau_x + \mathrm{e}^{-p}\sqrt{\frac{c}{2\alpha}}\right) \approx \ln\left(\mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{c}{2\alpha}}\right) \tag{A.4}$$

The approximation is valid when $\left(\mathrm{e}^{-d\sqrt{\frac{\alpha}{D}}}\sqrt{\frac{c}{2\alpha}}\right)$ is small, i.e., $\ln(1+x) \approx \ln(x)$ for x small. Thus by substituting (A.4) in (A.3) and by further solving we obtain the approximate expression

which is given as

$$C_{ub} \approx 1 + \ln(d) - \ln\left(\sqrt{4D\alpha}\right) \tag{A.5}$$

Appendix B

Mathematical Proofs

B.1 Proof of eq. (5.11)

Let us recall the GSOP expression, which can be written as follows

$$\begin{aligned} P_{out} =& \mathbb{P}(M_E \geq \lambda_2) + \mathbb{P}(\lambda_1 < M_E < \lambda_2) \times \mathbb{P}\left(\frac{AR_B - 2\ln(M_E) - B}{AR_S} < \phi \middle| \lambda_1 < M_E < \lambda_2 \right) \\ =& \mathbb{P}(M_E \geq \lambda_2) + X \\ =& \int_{\lambda_2}^{\infty} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \, dm + X, \end{aligned} \tag{B.1}$$

where X is given as

$$\begin{aligned} X &= \mathbb{P}(\lambda_1 < M_E < \lambda_2) \times \mathbb{P}\left(\frac{AR_B - 2\ln(M_E) - B}{AR_S} < \phi \middle| \lambda_1 < M_E < \lambda_2 \right) \\ &= \mathbb{P}(\lambda_1 < M_E < \lambda_2) \times \mathbb{P}\left(M_E > \mathrm{e}^{\frac{A(R_B - R_S\phi) - B}{2}} \middle| \lambda_1 < M_E < \lambda_2 \right) \\ &= \mathbb{P}(\lambda_1 < M_E < \lambda_2) \times \frac{\mathbb{P}\left(\mathrm{e}^{\frac{A(R_B - R_S\phi) - B}{2}} < M_E < \lambda_2 \right)}{\mathbb{P}(\lambda_1 < M_E < \lambda_2)} \\ &= \mathbb{P}\left(\mathrm{e}^{\frac{A(R_B - R_S\phi) - B}{2}} < M_E < \lambda_2 \right) \\ &= \int_{\mathrm{e}^{\frac{A(R_B - R_S\phi) - B}{2}}}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \, dm. \end{aligned} \tag{B.2}$$

Therefore, by substituting (B.2) in (B.1), the GSOP expression is obtained as

$$\begin{aligned} P_{out} &= \int_{\lambda_2}^{\infty} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm + \int_{\mathrm{e}^{\frac{A(R_B-R_S\phi)-B}{2}}}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm \\ &= Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right) + Q\left(\frac{\mathrm{e}^{\frac{A(R_B-R_S\phi)-B}{2}}-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right) \\ &= Q\left(\frac{\mathrm{e}^{\frac{A(R_B-R_S\phi)-B}{2}}-\mu_M}{\sigma_M}\right). \end{aligned} \tag{B.3}$$

B.2 Proof of eq. (5.16)

First we recall the expression of AFE in (5.15), which can be represented as

$$\begin{aligned} \bar{\Delta} = &\int_0^{\lambda_1} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm + \int_{\lambda_1}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \left(\frac{AR_B-B}{AR_S}\right) dm \\ &- \int_{\lambda_1}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \left(\frac{2\ln(m)}{AR_S}\right) dm. \end{aligned} \tag{B.4}$$

By using the approximation of $\ln(m) \leq (am^{(\frac{1}{a})} - a)$ from [206, eq.4.1.37], the $\bar{\Delta}$ of (5.15) becomes

$$\begin{aligned} \bar{\Delta} = 1 &- Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) \\ &+ \left(\frac{AR_B-B}{AR_S}\right)\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\} \\ &- \int_{\lambda_1}^{\lambda_2} \frac{2a(m^{\frac{1}{a}}-1)}{AR_S\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm. \end{aligned} \tag{B.5}$$

Note that the approximation hold good for a>1. In this case we have taken a=100. Using above approximation the expression for average fractional equivocation is given by

$$\begin{aligned} \bar{\Delta} = 1 &- Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) \\ &+ \left(\frac{AR_B-B}{AR_S}\right)\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\} - F_1. \end{aligned} \tag{B.6}$$

where F_1 can be written as

$$F_1 = \int_{\lambda_1}^{\lambda_2} \frac{2a(m^{\frac{1}{a}})}{AR_S\sqrt{2\pi\sigma_M^2}} e^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm - \int_{\lambda_1}^{\lambda_2} \frac{2a}{AR_S\sqrt{2\pi\sigma_M^2}} e^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm \tag{B.7}$$

$$= \int_{\lambda_1}^{\lambda_2} \frac{2a(m^{\frac{1}{a}})}{AR_S\sqrt{2\pi\sigma_M^2}} e^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm - \frac{2a}{AR_S}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\}. \tag{B.8}$$

By substituting $\frac{(m-\mu)^2}{2\sigma_M^2} = t$ we obtain

$$F_1 = \int_{t_1}^{t_2} \frac{ae^{-t}}{AR_S\sqrt{t\pi}}(\mu_M + \sqrt{2t\sigma_M^2})^{\frac{1}{a}}\, dt - \frac{2a}{AR_S}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\} \tag{B.9}$$

$$= \int_{t_1}^{t_2} \frac{a\mu_M^{\frac{1}{a}}e^{-t}}{AR_S\sqrt{t\pi}}\left(1 + \frac{\sqrt{2t\sigma_M^2}}{\mu_M}\right)^{\frac{1}{a}} dt - \frac{2a}{AR_S}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\}. \tag{B.10}$$

where $t_1 = \frac{(\lambda_1-\mu_M)^2}{2\sigma_M^2}$ and $t_2 = \frac{(\lambda_2-\mu_M)^2}{2\sigma_M^2}$. Now using the expansion given in [206, eq.3.6.9] the above integral can be modified as

$$F_1 = \int_{t_1}^{t_2} \frac{a\mu_M^{\frac{1}{a}}e^{-t}}{AR_S\sqrt{t\pi}}\left\{1 + \frac{\sqrt{2t\sigma_M^2}}{a\mu_M} + \frac{(1-a)(\sqrt{2t\sigma_M^2})^2}{2a^2\mu_M^2} + \frac{(1-a)(1-2a)(\sqrt{2t\sigma_M^2})^3}{6a^3\mu_M^3} + \ldots\right\} dt$$
$$- \frac{2a}{AR_S}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\}. \tag{B.11}$$

Using various integral properties, the above integral can be simplified to

$$F_1 = \left\{\frac{a\mu_M^{\frac{1}{a}}}{(AR_S)\sqrt{\pi}}\sqrt{\pi}\mathrm{erf}(\sqrt{t_2}) - \frac{a\mu_M^{\frac{1}{a}}}{(AR_S)\sqrt{\pi}}\sqrt{\pi}\mathrm{erf}(\sqrt{t_1}) + \frac{\sqrt{2\sigma_M^2}}{(AR_S)a\mu_M}\left(e^{-t_1} - e^{-t_2}\right) + O\right\}$$
$$- \frac{2a}{AR_S}\left(Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right). \tag{B.12}$$

where O represents other higher order terms. In the above expression the value of a is taken to be 100 to achieve accuracy on the approximation and to simultaneously neglect the other higher order terms in the series expansion. Therefore, by using (B.12) and organizing the terms we obtain (5.16).

B.3 Proof of eq. (5.23)

First, we recall the expression of $\mathbb{E}[\Delta^2]$ which is

$$\begin{aligned}\mathbb{E}[\Delta^2] &= \int_0^{\lambda_1} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm + \int_{\lambda_1}^{\lambda_2} \frac{(AR_B - 2\ln(m) - B)^2}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm \\ &= 1 - Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) + \int_{\lambda_1}^{\lambda_2} \frac{1}{\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}} \left(\frac{(AR_B - B)^2}{(AR_S)^2}\right) dm \\ &\quad + \int_{\lambda_1}^{\lambda_2} \frac{4\ln(m)\ln(m)}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm - \int_{\lambda_1}^{\lambda_2} \frac{4(AR_B - B)\ln(m)}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm.\end{aligned} \tag{B.13}$$

By using the integral properties and some algebraic operations the expression for the second moment of fractional equivocation is obtained as

$$\begin{aligned}\mathbb{E}[\Delta^2] = 1 - Q\left(\frac{\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right) + \frac{(AR_B - B)^2}{(AR_S)^2}\left\{Q\left(\frac{\lambda_1 - \mu_M}{\sigma_M}\right)\right\} \\ - \frac{(AR_B - B)^2}{(AR_S)^2}\left\{Q\left(\frac{\lambda_2 - \mu_M}{\sigma_M}\right)\right\} + F_2 - \frac{4(AR_B - B)}{(AR_S)^2} F_1,\end{aligned} \tag{B.14}$$

where F_1 is obtained from (B.12) and F_2 is given as

$$F_2 = \int_{\lambda_1}^{\lambda_2} \frac{4\ln(m)\ln(m)}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm. \tag{B.15}$$

Now by using $\ln(m) \leq (am^{\frac{1}{a}} - a)$ approximation the above integral becomes

$$\begin{aligned}F_2 &= \int_{\lambda_1}^{\lambda_2} \frac{4(am^{\frac{1}{a}} - a)^2}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm = \int_{\lambda_1}^{\lambda_2} \frac{4a^2 m^{\frac{2}{a}}}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm \\ &\quad + \int_{\lambda_1}^{\lambda_2} \frac{4a^2}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm - \int_{\lambda_1}^{\lambda_2} \frac{8a^2 m^{\frac{1}{a}}}{(AR_S)^2\sqrt{2\pi\sigma_M^2}} \mathrm{e}^{-\frac{(m-\mu_M)^2}{2\sigma_M^2}}\, dm.\end{aligned} \tag{B.16}$$

By substituting $\frac{(m-\mu)^2}{2\sigma_M^2} = t$ and using the expansion given in [206, eq.3.6.9] the above integral can further be simplified to

$$F_2 = \int_{t_1}^{t_2} \frac{4a^2 e^{-t}}{2(AR_S)^2\sqrt{t\pi}} (\mu_M + \sqrt{2t\sigma_M^2})^{\frac{2}{a}}\, dt + \frac{4a^2}{(AR_S)^2}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\}$$
$$-\frac{4a^2}{(AR_S)^2}\left\{\frac{a\mu_M^{\frac{1}{a}}}{\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_2}) - \frac{a\mu_M^{\frac{1}{a}}}{\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_1}) + \frac{\sqrt{2\sigma_M^2}}{a\mu_M}\left(e^{-t_1} - e^{-t_2}\right) + O\right\}. \tag{B.17}$$

where $t_1 = \frac{(\lambda_1-\mu_M)^2}{2\sigma_M^2}$, $t_2 = \frac{(\lambda_2-\mu_M)^2}{2\sigma_M^2}$ and O represents other higher order terms. Now using the expansion given in [206, eq.3.6.9] the above integral can be modified as

$$F_2 = \int_{t_1}^{t_2} \frac{4a^2\mu_M^{\frac{2}{a}} e^{-t}}{2(AR_S)^2\sqrt{t\pi}}\left\{1 + \frac{2\sqrt{2t\sigma_M^2}}{a\mu_M} + \frac{2(2-a)(\sqrt{2t\sigma_M^2})^2}{2a^2\mu_M^2} + ...\right\} dt$$
$$+\frac{4a^2}{(AR_S)^2}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\} - \frac{4a}{(AR_S)^2}\left\{\frac{a\mu_M^{\frac{1}{a}}}{\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_2})\right.$$
$$\left. - \frac{a\mu_M^{\frac{1}{a}}}{\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_1}) + \frac{\sqrt{2\sigma_M^2}}{a\mu_M}\left(e^{-t_1} - e^{-t_2}\right) + O\right\}. \tag{B.18}$$

By using various integral properties, the above integral can be rewritten as

$$F_2 = \left\{\frac{4a^2\mu_M^{\frac{2}{a}}}{(AR_S)^2\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_2}) - \frac{4a^2\mu_M^{\frac{2}{a}}}{(AR_S)^2\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_1}) + \frac{4a^2\mu_M^{\frac{2}{a}}\sqrt{2\sigma_M^2}}{(AR_S)^2 a\mu_M}\left(e^{-t_1} - e^{-t_2}\right) + O\right\}$$
$$+\frac{4a^2}{(AR_S)^2}\left\{Q\left(\frac{\lambda_1-\mu_M}{\sigma_M}\right) - Q\left(\frac{\lambda_2-\mu_M}{\sigma_M}\right)\right\} - \frac{4a}{(AR_S)^2}\left\{\frac{a\mu_M^{\frac{1}{a}}}{\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_2})\right.$$
$$\left. - \frac{a\mu_M^{\frac{1}{a}}}{\sqrt{\pi}}\sqrt{\pi}\text{erf}(\sqrt{t_1}) + \frac{\sqrt{2\sigma_M^2}}{a\mu_M}\left(e^{-t_1} - e^{-t_2}\right) + O\right\}. \tag{B.19}$$

In the above expression, the value of a is taken to be 100 to achieve accuracy on the approximation and to neglect the other higher-order terms in the series expansion simultaneously. Using (B.12) and (B.19), with subsequent rearranging the terms, we obtain (5.23).

References

[1] T. Nakano, A. W. Eckford, and T. Haraguchi, *Molecular communication*. Cambridge University Press, 2013.

[2] M. Stojanovic, "Acoustic (underwater) communications," *Wiley Encyclopedia of Telecommunications*, 2003.

[3] R. A. Freitas, *Nanomedicine, volume I: basic capabilities*. Landes Bioscience Georgetown, TX, 1999, vol. 1.

[4] S. Sengupta, M. E. Ibele, and A. Sen, "Fantastic voyage: designing self-powered nanorobots," *Angewandte Chemie International Edition*, vol. 51, no. 34, pp. 8434–8445, 2012.

[5] W. Guo, C. Mias, N. Farsad, and J.-L. Wu, "Molecular versus electromagnetic wave propagation loss in macro-scale environments," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 1, pp. 18–25, 2015.

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

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

[8] A. Gohari, M. Mirmohseni, and M. Nasiri-Kenari, "Information theory of molecular communication: Directions and challenges," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 2, no. 2, pp. 120–142, 2016.

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

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

[11] B. Alberts, A. Johnson, J. Lewis, M. Raff, K. Roberts, P. Walter *et al.*, "Molecular biology of the cell," *SCANDINAVIAN JOURNAL OF RHEUMATOLOGY*, vol. 32, no. 2, pp. 125–125, 2003.

[12] W. C. Agosta, *Chemical communication: the language of pheromones*. Henry Holt and Company, 1992.

[13] M. S. Kuran, H. B. Yilmaz, T. Tugcu, and I. F. Akyildiz, "Modulation techniques for communication via diffusion in nanonetworks," in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1–5.

[14] N. Pandey, R. K. Mallik, and B. Lall, "Molecular communication: The first arrival position channel," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 508–511, 2018.

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

[16] T. Nakano, T. Suda, T. Koujin, T. Haraguchi, and Y. Hiraoka, "Molecular communication through gap junction channels," in *Transactions on Computational Systems Biology X*. Springer, 2008, pp. 81–99.

[17] K. V. Srinivas, A. W. Eckford, and R. S. Adve, "Molecular communication in fluid media: The additive inverse gaussian noise channel," *IEEE transactions on information theory*, vol. 58, no. 7, pp. 4678–4692, 2012.

[18] A. Enomoto, M. J. Moore, T. Suda, and K. Oiwa, "Design of self-organizing microtubule networks for molecular communication," *Nano Communication Networks*, vol. 2, no. 1, pp. 16–24, 2011.

[19] J. Crank, *The mathematics of diffusion*. Oxford university press, 1979.

[20] B. Alberts, A. Johnson, J. Lewis, D. Morgan, M. Raff, K. Roberts, P. Walter, J. Wilson, and T. Hunt, *Molecular biology of the cell*. WW Norton & Company, 2017.

[21] H. C. Berg, *Random walks in biology*. Princeton University Press, 2018.

[22] P. Cuatrecasas, "Membrane receptors," *Annual review of biochemistry*, vol. 43, no. 1, pp. 169–214, 1974.

[23] A. W. Eckford, "Nanoscale communication with brownian motion," in *2007 41st Annual Conference on Information Sciences and Systems*. IEEE, 2007, pp. 160–165.

[24] H. B. Yilmaz, A. C. Heren, T. Tugcu, and C.-B. Chae, "Three-dimensional channel characteristics for molecular communications with an absorbing receiver," *IEEE Communications Letters*, vol. 18, no. 6, pp. 929–932, 2014.

[25] S. Redner, *A guide to first-passage processes*. Cambridge University Press, 2001.

[26] D. L. L. Dy and J. Esguerra, "First-passage-time distribution for diffusion through a planar wedge," *Physical Review E*, vol. 78, no. 6, p. 062101, 2008.

[27] W. Hundsdorfer and J. G. Verwer, *Numerical solution of time-dependent advection-diffusion-reaction equations*. Springer Science & Business Media, 2013, vol. 33.

[28] A. Guha, "Transport and deposition of particles in turbulent and laminar flow," *Annu. Rev. Fluid Mech.*, vol. 40, pp. 311–341, 2008.

[29] C. Zoppou and J. Knight, "Analytical solution of a spatially variable coefficient advection–diffusion equation in up to three dimensions," *Applied Mathematical Modelling*, vol. 23, no. 9, pp. 667–685, 1999.

[30] S. Hiyama, Y. Moritani, R. Gojo, S. Takeuchi, and K. Sutoh, "Biomolecular-motor-based autonomous delivery of lipid vesicles as nano-or microscale reactors on a chip," *Lab on a Chip*, vol. 10, no. 20, pp. 2741–2748, 2010.

[31] S. F. Bush, *Nanoscale communication networks*. Artech House, 2010.

[32] S. Hiyama, R. Gojo, T. Shima, S. Takeuchi, and K. Sutoh, "Biomolecular-motor-based nano-or microscale particle translocations on dna microarrays," *Nano Letters*, vol. 9, no. 6, pp. 2407–2413, 2009.

[33] Z. Wang, M. Kim, and G. Rosen, "Validating models of bacterial chemotaxis by simulating the random motility coefficient," in *2008 8th IEEE International Conference on BioInformatics and BioEngineering*. IEEE, 2008, pp. 1–5.

[34] M. Kang and H. G. Othmer, "Spatiotemporal characteristics of calcium dynamics in astrocytes," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 3, p. 037116, 2009.

[35] M. Cole, J. Gardner, Z. Ráczu, S. Pathak, T. Pearce, J. Challiss, D. Markovic, A. Guerrero, L. Muñoz, G. Carot *et al.*, "Biomimetic insect infochemical communication system," in *SENSORS, 2009 IEEE*. IEEE, 2009, pp. 1358–1361.

[36] 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 *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[37] M. U. Mahfuz, D. Makrakis, and H. T. Mouftah, "On the characterization of binary concentration-encoded molecular communication in nanonetworks," *Nano Communication Networks*, vol. 1, no. 4, pp. 289–300, 2010.

[38] N.-R. Kim and C.-B. Chae, "Novel modulation techniques using isomers as messenger molecules for nano communication networks via diffusion," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 12, pp. 847–856, 2013.

[39] N. Garralda, I. Llatser, A. Cabellos-Aparicio, E. Alarcón, and M. Pierobon, "Diffusion-based physical channel identification in molecular nanonetworks," *Nano Communication Networks*, vol. 2, no. 4, pp. 196–204, 2011.

[40] Y.-P. Hsieh, Y.-C. Lee, P.-J. Shih, P.-C. Yeh, and K.-C. Chen, "On the asynchronous information embedding for event-driven systems in molecular communications," *Nano Communication Networks*, vol. 4, no. 1, pp. 2–13, 2013.

[41] B. Krishnaswamy, C. M. Austin, J. P. Bardill, D. Russakow, G. L. Holst, B. K. Hammer, C. R. Forest, and R. Sivakumar, "Time-elapse communication: Bacterial communication on a microfluidic chip," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5139–5151, 2013.

[42] B. Tepekule, A. E. Pusane, H. B. Yilmaz, and T. Tugcu, "Energy efficient isi mitigation for communication via diffusion," in *2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE, 2014, pp. 33–37.

[43] B. Atakan, S. Galmes, and O. B. Akan, "Nanoscale communication with molecular arrays in nanonetworks," *IEEE Transactions on NanoBioscience*, vol. 11, no. 2, pp. 149–160, 2012.

[44] H. Arjmandi, A. Gohari, M. N. Kenari, and F. Bateni, "Diffusion-based nanonetworking: A new modulation technique and performance analysis," *IEEE Communications Letters*, vol. 17, no. 4, pp. 645–648, 2013.

[45] M. Ş. Kuran, H. B. Yilmaz, T. Tugcu, and I. F. Akyildiz, "Interference effects on modulation techniques in diffusion based nanonetworks," *Nano Communication Networks*, vol. 3, no. 1, pp. 65–73, 2012.

[46] C. T. Chou, "Molecular circuits for decoding frequency coded signals in nano-communication networks," *Nano Communication Networks*, vol. 3, no. 1, pp. 46–56, 2012.

[47] H. ShahMohammadian, G. G. Messier, and S. Magierowski, "Optimum receiver for molecule shift keying modulation in diffusion-based molecular communication channels," *Nano Communication Networks*, vol. 3, no. 3, pp. 183–195, 2012.

[48] M. U. Mahfuz, D. Makrakis, and H. T. Mouftah, "A generalized strength-based signal detection model for concentration-encoded molecular communication," in *Proceedings of the 8th International Conference on Body Area Networks*, 2013, pp. 461–467.

[49] H. Kitano, "Computational systems biology," *Nature*, vol. 420, no. 6912, pp. 206–210, 2002.

[50] M. Hirabayashi, A. Nishikawa, F. Tanaka, M. Hagiya, H. Kojima, and K. Oiwa, "Design of molecular-based network robots-toward the environmental control," in *2011 11th IEEE International Conference on Nanotechnology*. IEEE, 2011, pp. 313–318.

[51] R. Chang, *Physical chemistry for the biosciences*. University Science Books, 2005.

[52] A. A. Requicha, "Nanorobots, nems, and nanoassembly," *Proceedings of the IEEE*, vol. 91, no. 11, pp. 1922–1933, 2003.

[53] K. Kostarelos, "Nanorobots for medicine: how close are we?" *Nanomedicine*, vol. 5, no. 3, pp. 341–342, 2010.

[54] S. P. Leary, C. Y. Liu, and M. Apuzzo, "Toward the emergence of nanoneurosurgery: part iii–nanomedicine: targeted nanotherapy, nanosurgery, and progress toward the realization of nanoneurosurgery." *Neurosurgery*, vol. 58, no. 6, pp. 1009–26, 2006.

[55] S. M. Douglas, I. Bachelet, and G. M. Church, "A logic-gated nanorobot for targeted transport of molecular payloads," *Science*, vol. 335, no. 6070, pp. 831–834, 2012.

[56] A. Cavalcanti, B. Shirinzadeh, T. Fukuda, and S. Ikeda, "Nanorobot for brain aneurysm," *The International Journal of Robotics Research*, vol. 28, no. 4, pp. 558–570, 2009.

[57] F. Stajano, N. Hoult, I. Wassell, P. Bennett, C. Middleton, and K. Soga, "Smart bridges, smart tunnels: Transforming wireless sensor networks from research prototypes into robust engineering infrastructure," *Ad Hoc Networks*, vol. 8, no. 8, pp. 872–888, 2010.

[58] R. K. Vander Meer, M. D. Breed, M. Winston, and K. E. Espelie, *Pheromone communication in social insects: ants, wasps, bees, and termites*. CRC Press, 2019.

[59] A. Einolghozati, M. Sardari, A. Beirami, and F. Fekri, "Capacity of discrete molecular diffusion channels," in *2011 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2011, pp. 723–727.

[60] A. Einolghozati, M. Sardari, and F. Fekri, "Capacity of diffusion-based molecular communication with ligand receptors," in *2011 IEEE Information Theory Workshop*. IEEE, 2011, pp. 85–89.

[61] D. Arifler, "Capacity analysis of a diffusion-based short-range molecular nanocommunication channel," *Computer Networks*, vol. 55, no. 6, pp. 1426–1434, 2011.

[62] H. B. Yilmaz and C.-B. Chae, "Arrival modelling for molecular communication via diffusion," *Electronics Letters*, vol. 50, no. 23, pp. 1667–1669, 2014.

[63] T. Nakano, Y. Okaie, and J.-Q. Liu, "Channel model and capacity analysis of molecular communication with brownian motion," *IEEE communications letters*, vol. 16, no. 6, pp. 797–800, 2012.

[64] M. Ş. Kuran, H. B. Yilmaz, T. Tugcu, and B. Özerman, "Energy model for communication via diffusion in nanonetworks," *Nano Communication Networks*, vol. 1, no. 2, pp. 86–95, 2010.

[65] M. Pierobon and I. F. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, pp. 602–611, 2010.

[66] ——, "Diffusion-based noise analysis for molecular communication in nanonetworks," *IEEE Transactions on signal processing*, vol. 59, no. 6, pp. 2532–2547, 2011.

[67] ——, "Capacity of a diffusion-based molecular communication system with channel memory and molecular noise," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 942–954, 2012.

[68] A. Einolghozati, M. Sardari, and F. Fekri, "Collective sensing-capacity of bacteria populations," in *2012 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2012, pp. 2959–2963.

[69] ——, "Design and analysis of wireless communication systems using diffusion-based molecular communication among bacteria," *IEEE transactions on wireless communications*, vol. 12, no. 12, pp. 6096–6105, 2013.

[70] A. Guney, B. Atakan, and O. B. Akan, "Mobile ad hoc nanonetworks with collision-based molecular communication," *IEEE Transactions on Mobile Computing*, vol. 11, no. 3, pp. 353–366, 2011.

[71] C. T. Chou, "Extended master equation models for molecular communication networks," *IEEE transactions on nanobioscience*, vol. 12, no. 2, pp. 79–92, 2013.

[72] D. Miorandi, "A stochastic model for molecular communications," *Nano Communication Networks*, vol. 2, no. 4, pp. 205–212, 2011.

[73] N. Farsad, A. W. Eckford, and S. Hiyama, "A markov chain channel model for active transport molecular communication," *IEEE Transactions on Signal Processing*, vol. 62, no. 9, pp. 2424–2436, 2014.

[74] N. Farsad, A. W. Eckford, S. Hiyama, and Y. Moritani, "On-chip molecular communication: Analysis and design," *IEEE Transactions on NanoBioscience*, vol. 11, no. 3, pp. 304–314, 2012.

[75] A. C. Heren, M. Ş. Kuran, H. B. Yilmaz, and T. Tugcu, "Channel capacity of calcium signalling based on inter-cellular calcium waves in astrocytes," in *2013 IEEE International Conference on Communications Workshops (ICC)*. IEEE, 2013, pp. 792–797.

[76] D. Kilinc and O. B. Akan, "An information theoretical analysis of nanoscale molecular gap junction communication channel between cardiomyocytes," *IEEE Transactions on Nanotechnology*, vol. 12, no. 2, pp. 129–136, 2012.

[77] Y. Chahibi, M. Pierobon, S. O. Song, and I. F. Akyildiz, "A molecular communication system model for particulate drug delivery systems," *IEEE Transactions on biomedical engineering*, vol. 60, no. 12, pp. 3468–3483, 2013.

[78] A. O. Bicen and I. F. Akyildiz, "System-theoretic analysis and least-squares design of microfluidic channels for flow-induced molecular communication," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 5000–5013, 2013.

[79] I. Mian and C. Rose, "Communication theory and multicellular biology," *Integrative Biology*, vol. 3, no. 4, pp. 350–367, 2011.

[80] N. Pandey, R. K. Mallik, and B. Lall, "Truncated lévy statistics for diffusion based molecular communication," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[81] N. Farsad, W. Guo, C. Chae, and A. Eckford, "Stable distributions as noise models for molecular communication," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–6.

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

[83] N. Farsad, Y. Murin, A. Eckford, and A. Goldsmith, "On the capacity of diffusion-based molecular timing channels," in *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2016, pp. 1023–1027.

[84] S. M. Riazul Islam, F. Ali, H. Moon, and K. Kwak, "Secure channel for molecular communications," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 2017, pp. 1–4.

[85] R. P. Feynman *et al.*, "There's plenty of room at the bottom," *California Institute of Technology, Engineering and Science magazine*, 1960.

[86] T. Nakano, T. Suda, M. Moore, R. Egashira, A. Enomoto, and K. Arima, "Molecular communication for nanomachines using intercellular calcium signaling," in *5th IEEE Conference on Nanotechnology, 2005.* IEEE, 2005, pp. 478–481.

[87] G. Alfano and D. Miorandi, "On information transmission among nanomachines," in *2006 1st International Conference on Nano-Networks and Workshops*. IEEE, 2006, pp. 1–5.

[88] P. J. Thomas, D. J. Spencer, S. K. Hampton, P. Park, and J. P. Zurkus, "The diffusion-limited biochemical signal-relay channel," in *Advances in Neural Information Processing Systems*. Citeseer, 2004, pp. 1263–1270.

[89] B. Atakan and O. B. Akan, "An information theoretical approach for molecular communication," in *2007 2nd Bio-Inspired Models of Network, Information and Computing Systems*. IEEE, 2007, pp. 33–40.

[90] T. Nakano, T. Suda, T. Koujin, T. Haraguchi, and Y. Hiraoka, "Molecular communication through gap junction channels: System design, experiments and modeling," in *2007 2nd Bio-Inspired Models of Network, Information and Computing Systems*. IEEE, 2007, pp. 139–146.

[91] M. Gregori and I. F. Akyildiz, "A new nanonetwork architecture using flagellated bacteria and catalytic nanomotors," *IEEE Journal on selected areas in communications*, vol. 28, no. 4, pp. 612–619, 2010.

[92] M. Gregori, I. Llatser, A. Cabellos-Aparicio, and E. Alarcón, "Physical channel characterization for medium-range nanonetworks using flagellated bacteria," *Computer Networks*, vol. 55, no. 3, pp. 779–791, 2011.

[93] M. Moore, A. Enomoto, T. Nakano, R. Egashira, T. Suda, A. Kayasuga, H. Kojima, H. Sakakibara, and K. Oiwa, "A design of a molecular communication system for nanomachines using molecular motors," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*. IEEE, 2006, pp. 6–pp.

[94] M. J. Moore, T. Suda, and K. Oiwa, "Molecular communication: Modeling noise effects on information rate," *IEEE transactions on nanobioscience*, vol. 8, no. 2, pp. 169–180, 2009.

[95] C. Bustamante, D. Keller, and G. Oster, "The physics of molecular motors," *Accounts of chemical research*, vol. 34, no. 6, pp. 412–420, 2001.

[96] S. Kadloor and R. Adve, "A framework to study the molecular communication system," in *2009 Proceedings of 18th International Conference on Computer Communications and Networks*. IEEE, 2009, pp. 1–6.

[97] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[98] A. W. Eckford, "Achievable information rates for molecular communication with distinct molecules," in *2007 2nd Bio-Inspired Models of Network, Information and Computing Systems*. IEEE, 2007, pp. 313–315.

[99] M. J. Moore, A. Enomoto, T. Suda, A. Kayasuga, and K. Oiwa, "Molecular communication: uni-cast communication on a microtubule topology," in *2008 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2008, pp. 18–23.

[100] G. Battail, "Heredity as an encoded communication process," *IEEE transactions on information theory*, vol. 56, no. 2, pp. 678–687, 2010.

[101] T. Nakano and J.-Q. Liu, "Design and analysis of molecular relay channels: An information theoretic approach," *IEEE Transactions on NanoBioscience*, vol. 9, no. 3, pp. 213–221, 2010.

[102] L. Gong, N. Bouaynaya, and D. Schonfeld, "Information-theoretic model of evolution over protein communication channel," *IEEE/ACM transactions on computational biology and bioinformatics*, vol. 8, no. 1, pp. 143–151, 2009.

[103] M. Pierobon and I. F. Akyildiz, "Noise analysis in ligand-binding reception for molecular communication in nanonetworks," *IEEE Transactions on Signal Processing*, vol. 59, no. 9, pp. 4168–4182, 2011.

[104] H.-T. Chang and S. M. Moser, "Bounds on the capacity of the additive inverse gaussian noise channel," in *2012 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2012, pp. 299–303.

[105] H. Li, S. M. Moser, and D. Guo, "Capacity of the memoryless additive inverse gaussian noise channel," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 12, pp. 2315–2329, 2014.

[106] A. W. Eckford, K. Srinivas, and R. S. Adve, "The peak constrained additive inverse gaussian noise channel," in *2012 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2012, pp. 2973–2977.

[107] H. Qian and S. Roy, "An information theoretical analysis of kinase activated phosphorylation dephosphorylation cycle," *IEEE transactions on nanobioscience*, vol. 11, no. 3, pp. 289–295, 2012.

[108] B. Atakan, "Optimal transmission probability in binary molecular communication," *IEEE communications letters*, vol. 17, no. 6, pp. 1152–1155, 2013.

[109] T. Nakano, Y. Okaie, and J. Liu, "Channel model and capacity analysis of molecular communication with brownian motion," *IEEE Communications Letters*, vol. 16, no. 6, pp. 797–800, 2012.

[110] F. Balado, "Capacity of dna data embedding under substitution mutations," *IEEE transactions on information theory*, vol. 59, no. 2, pp. 928–941, 2012.

[111] P.-J. Shih, C.-H. Lee, P.-C. Yeh, and K.-C. Chen, "Channel codes for reliability enhancement in molecular communication," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 12, pp. 857–867, 2013.

[112] S. F. Bush and S. Goel, "Persistence length as a metric for modeling and simulation of nanoscale communication networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 12, pp. 815–824, 2013.

[113] A. Noel, K. C. Cheung, and R. Schober, "Improving receiver performance of diffusive molecular communication with enzymes," *IEEE Transactions on NanoBioscience*, vol. 13, no. 1, pp. 31–43, 2014.

[114] M. T. Barros, S. Balasubramaniam, and B. Jennings, "Using information metrics and molecular communication to detect cellular tissue deformation," *IEEE transactions on nanobioscience*, vol. 13, no. 3, pp. 278–288, 2014.

[115] Y. Chahibi and I. F. Akyildiz, "Molecular communication noise and capacity analysis for particulate drug delivery systems," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 3891–3903, 2014.

[116] A. O. Bicen and I. F. Akyildiz, "Interference modeling and capacity analysis for microfluidic molecular communication channels," *IEEE Transactions on Nanotechnology*, vol. 14, no. 3, pp. 570–579, 2015.

[117] N. Michelusi and U. Mitra, "Capacity of electron-based communication over bacterial cables: the full-csi case," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 1, pp. 62–75, 2015.

[118] M. T. Barros, S. Balasubramaniam, and B. Jennings, "Comparative end-to-end analysis of ca 2+-signaling-based molecular communication in biological tissues," *IEEE Transactions on Communications*, vol. 63, no. 12, pp. 5128–5142, 2015.

[119] K. Mehta and J. Kliewer, "An information theoretic approach toward assessing perceptual audio quality using eeg," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 2, pp. 176–187, 2015.

[120] S. Ghavami, R. S. Adve, and F. Lahouti, "Information rates of ask-based molecular communication in fluid media," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 3, pp. 277–291, 2015.

[121] B.-H. Koo, C. Lee, H. B. Yilmaz, N. Farsad, A. Eckford, and C.-B. Chae, "Molecular mimo: From theory to prototype," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 600–614, 2016.

[122] A. Einolghozati and F. Fekri, "Analysis of error-detection schemes in diffusion-based molecular communication," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 615–624, 2016.

[123] P. J. Thomas and A. W. Eckford, "Capacity of a simple intercellular signal transduction channel," *IEEE Transactions on information Theory*, vol. 62, no. 12, pp. 7358–7382, 2016.

[124] P. A. Iglesias, "The use of rate distortion theory to evaluate biological signaling pathways," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 2, no. 1, pp. 31–39, 2016.

[125] V. Loscrí and A. M. Vegni, "Capacity evaluation of a quantum-based channel in a biological context," *IEEE transactions on nanobioscience*, vol. 15, no. 8, pp. 901–907, 2016.

[126] L. R. Varshney, J. Kusuma, and V. K. Goyal, "On palimpsests in neural memory: An information theory viewpoint," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 2, no. 2, pp. 143–153, 2016.

[127] S. M. Mustam, S. K. Syed-Yusof, and S. Zubair, "Capacity and delay spread in multi-layer diffusion-based molecular communication (dbmc) channel," *IEEE transactions on nanobioscience*, vol. 15, no. 7, pp. 599–612, 2016.

[128] C. Rose and I. S. Mian, "Inscribed matter communication: Part ii," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 2, no. 2, pp. 228–239, 2016.

[129] ——, "Inscribed matter communication: Part i," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 2, no. 2, pp. 209–227, 2016.

[130] M. Sungkar, T. Berger, and W. B. Levy, "Mutual information and parameter estimation in the generalized inverse gaussian diffusion model of cortical neurons," *IEEE Transactions*

on Molecular, Biological and Multi-Scale Communications, vol. 2, no. 2, pp. 166–182, 2016.

[131] H. Arjmandi, M. Movahednasab, A. Gohari, M. Mirmohseni, M. Nasiri-Kenari, and F. Fekri, "Isi-avoiding modulation for diffusion-based molecular communication," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 3, no. 1, pp. 48–59, 2016.

[132] M. L. De Freitas, M. Egan, L. Clavier, A. Goupil, G. W. Peters, and N. Azzaoui, "Capacity bounds for additive symmetric α-stable noise channels," *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5115–5123, 2017.

[133] N. A. Abbasi and O. B. Akan, "An information theoretical analysis of human insulin-glucose system toward the internet of bio-nano things," *IEEE transactions on nanobioscience*, vol. 16, no. 8, pp. 783–791, 2017.

[134] A. O. Bicen, J. J. Lehtomäki, and I. F. Akyildiz, "Shannon meets fick on the microfluidic channel: Diffusion limit to sum broadcast capacity for molecular communication," *IEEE transactions on nanobioscience*, vol. 17, no. 1, pp. 88–94, 2018.

[135] V. Loscrí, B. D. Unluturk, and A. M. Vegni, "A molecular optical channel model based on phonon-assisted energy transfer phenomenon," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6247–6259, 2018.

[136] H. Ghourchian, G. Aminian, A. Gohari, M. Mirmohseni, and M. Nasiri-Kenari, "On the capacity of a class of signal-dependent noise channels," *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7828–7846, 2018.

[137] B. A. Bilgin, E. Dinc, and O. B. Akan, "Dna-based molecular communications," *IEEE Access*, vol. 6, pp. 73 119–73 129, 2018.

[138] N. Varshney, W. Haselmayr, and W. Guo, "On flow-induced diffusive mobile molecular communication: First hitting time and performance analysis," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 4, no. 4, pp. 195–207, 2018.

[139] L. Feng, Q. Yang, D. Park, and K. S. Kwak, "Energy efficient nano-node association and resource allocation for hierarchical nano-communication networks," *IEEE Transactions*

on Molecular, Biological and Multi-Scale Communications, vol. 4, no. 4, pp. 208–220, 2018.

[140] H. Awan, R. S. Adve, N. Wallbridge, C. Plummer, and A. W. Eckford, "Communication and information theory of single action potential signals in plants," *IEEE transactions on nanobioscience*, vol. 18, no. 1, pp. 61–73, 2018.

[141] T. V. Martins, J. Hammelman, S. Marinova, C. O. Ding, and R. J. Morris, "An information-theoretical approach for calcium signaling specificity," *IEEE transactions on nanobioscience*, vol. 18, no. 1, pp. 93–100, 2018.

[142] D. T. McGuiness, S. Giannoukos, A. Marshall, and S. Taylor, "Modulation analysis in macro-molecular communications," *IEEE Access*, vol. 7, pp. 11 049–11 065, 2019.

[143] A. Etemadi, H. Arjmandi, P. Azmi, and N. Mokari, "Capacity bounds for diffusive molecular communication over discrete-time compound poisson channels," *IEEE Communications Letters*, vol. 23, no. 5, pp. 793–796, 2019.

[144] C. Rose, I. S. Mian, and M. Ozmen, "Capacity bounds on point-to-point communication using molecules," *Proceedings of the IEEE*, vol. 107, no. 7, pp. 1342–1355, 2019.

[145] I. F. Akyildiz, M. Pierobon, and S. Balasubramaniam, "An information theoretic framework to analyze molecular communication systems based on statistical mechanics," *Proceedings of the IEEE*, vol. 107, no. 7, pp. 1230–1255, 2019.

[146] J. Sun and H. Li, "On the iid capacity-achieving input for binding channels with multiple ligand receptors," *IEEE Access*, vol. 7, pp. 104 380–104 393, 2019.

[147] H. Awan, R. S. Adve, N. Wallbridge, C. Plummer, and A. W. Eckford, "Information theoretic based comparative analysis of different communication signals in plants," *IEEE Access*, vol. 7, pp. 117 075–117 087, 2019.

[148] T. Nakano, L. Lin, Y. Okaie, C. Wu, H. Yan, T. Hara, and K. Harumoto, "Random cell motion enhances the capacity of cell-cell communication," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 5, no. 2, pp. 158–162, 2019.

[149] M. Veletić and I. Balasingham, "An information theory of neuro-transmission in multiple-access synaptic channels," *IEEE Transactions on Communications*, vol. 68, no. 2, pp. 841–853, 2019.

[150] A. O. Kislal, B. C. Akdeniz, C. Lee, A. E. Pusane, T. Tugcu, and C.-B. Chae, "Isi-mitigating channel codes for molecular communication via diffusion," *IEEE Access*, vol. 8, pp. 24 588–24 599, 2020.

[151] U. A. Chude-Okonkwo, B. Maharaj, A. Vasilakos, and R. Malekian, "Information-theoretic model and analysis of molecular signaling in targeted drug delivery," *IEEE transactions on nanobioscience*, vol. 19, no. 2, pp. 270–284, 2020.

[152] Y. Okaie and T. Nakano, "Mobile molecular communication through multiple measurements of the concentration of molecules," *IEEE Access*, vol. 8, pp. 179 606–179 615, 2020.

[153] C.-L. Tai and I. F. Akyildiz, "A novel framework for capacity analysis of diffusion-based molecular communication incorporating chemical reactions," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 3, pp. 233–243, 2020.

[154] P. Lu, M. Veletić, J. Bergsland, and I. Balasingham, "Molecular communication aspects of potassium intracellular signaling in cardiomyocytes," *IEEE Access*, vol. 8, pp. 201 770–201 780, 2020.

[155] H. Awan, R. S. Adve, N. Wallbridge, C. Plummer, and A. W. Eckford, "Modelling the role of inter-cellular communication in modulating photosynthesis in plants," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2021.

[156] M. Ahuja, M. R. Bhatnagar *et al.*, "Markov chain modeling of the end-to-end molecular communication system using ligand receiver," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2021.

[157] M. Abbaszadeh, Y. Huang, P. J. Thomas, M. Wen, F. Ji, and W. Guo, "Kolmogorov turbulence and information dissipation in molecular communication," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2021.

[158] A. Borst and F. E. Theunissen, "Information theory and neural coding," *Nature neuroscience*, vol. 2, no. 11, pp. 947–957, 1999.

[159] V. Anantharam and S. Verdu, "Bits through queues," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 4–18, 1996.

[160] R. Sundaresan and S. Verdú, "Capacity of queues via point-process channels," *IEEE transactions on information theory*, vol. 52, no. 6, pp. 2697–2709, 2006.

[161] ——, "Robust decoding for timing channels," *IEEE Transactions on information Theory*, vol. 46, no. 2, pp. 405–419, 2000.

[162] C. Rose and I. S. Mian, "Signaling with identical tokens: Upper bounds with energy constraints," in *2014 IEEE International Symposium on Information Theory*. IEEE, 2014, pp. 1817–1821.

[163] R. Chhikara, *The inverse Gaussian distribution: theory: methodology, and applications*. CRC Press, 1988, vol. 95.

[164] Y. Murin, N. Farsad, M. Chowdhury, and A. Goldsmith, "Time-slotted transmission over molecular timing channels," *Nano communication networks*, vol. 12, pp. 12–24, 2017.

[165] N. Farsad, Y. Murin, A. W. Eckford, and A. Goldsmith, "Capacity limits of diffusion-based molecular timing channels with finite particle lifetime," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 4, no. 2, pp. 88–106, 2018.

[166] A. Einolghozati, M. Sardari, A. Beirami, and F. Fekri, "Capacity of discrete molecular diffusion channels," in *2011 IEEE International Symposium on Information Theory Proceedings*. IEEE, jul 2011.

[167] S. Aeeneh, N. Zlatanov, A. Gohari, M. Nasiri-Kenari, and M. Mirmohseni, "Timing modulation for macro-scale molecular communication," *IEEE Wireless Communications Letters*, vol. 9, no. 9, pp. 1356–1360, 2020.

[168] J. Lee, M. Kim, and D.-H. Cho, "Asynchronous detection algorithm for diffusion-based molecular communication in timing modulation channel," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2114–2117, 2015.

[169] Y. Murin, N. Farsad, M. Chowdhury, and A. Goldsmith, "Exploiting diversity in one-shot molecular timing channels via order statistics," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 4, no. 1, pp. 14–26, 2018.

[170] B. C. Akdeniz, A. E. Pusane, and T. Tugcu, "Position-based modulation in molecular communications," *Nano communication networks*, vol. 16, pp. 60–68, 2018.

[171] N. Farsad, Y. Murin, W. Guo, C.-B. Chae, A. W. Eckford, and A. Goldsmith, "Communication system design and analysis for asynchronous molecular timing channels," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 3, no. 4, pp. 239–253, 2017.

[172] G. D. Ntouni, V. M. Kapinas, and G. K. Karagiannidis, "On the optimal timing of detection in molecular communication systems," in *2017 24th International Conference on Telecommunications (ICT)*. IEEE, 2017, pp. 1–5.

[173] ——, "Optimization of the detection process timing in molecular communication systems with flow," in *2017 25th Telecommunication Forum (TELFOR)*. IEEE, 2017, pp. 1–4.

[174] Y. Murin, M. Chowdhury, N. Farsad, and A. Goldsmith, "Diversity gain of one-shot communication over molecular timing channels," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[175] N. Farsad, Y. Murin, W. Guo, C.-B. Chae, A. Eckford, and A. Goldsmith, "On the impact of time-synchronization in molecular timing channels," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[176] M. Egan, Y. Deng, M. Elkashlan, and T. Q. Duong, "Variance-constrained capacity of the molecular timing channel with synchronization error," in *2014 IEEE Global Communications Conference*. IEEE, 2014, pp. 1473–1478.

[177] M. Kovačević and P. Popovski, "Zero-error capacity of a class of timing channels," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6796–6800, 2014.

[178] N. Farsad, Y. Murin, M. Rao, and A. Goldsmith, "On the capacity of diffusion-based molecular timing channels with diversity," in *2016 50th Asilomar Conference on Signals, Systems and Computers*. IEEE, 2016, pp. 1117–1121.

[179] C. Rose and I. S. Mian, "A fundamental framework for molecular communication channels: Timing & payload," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 1043–1048.

[180] Y. Murin, N. Farsad, M. Chowdhury, and A. Goldsmith, "Optimal detection for one-shot transmission over diffusion-based molecular timing channels," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 4, no. 2, pp. 43–60, 2018.

[181] J. Xiong and H. Li, "Receiver design for binary timing-based molecular communication," in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*. IEEE, 2016, pp. 1–6.

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

[183] 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. 110 687–110 697, 2019.

[184] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3416–3430, 2017.

[185] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE transactions on nanobioscience*, vol. 13, no. 3, pp. 198–207, 2014.

[186] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 665–676, 2015.

[187] W. Guo, Z. Wei, and B. Li, "Secure internet-of-nano things for targeted drug delivery: Distance-based molecular cipher keys," in *2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME)*, 2020, pp. 1–6.

[188] W. Guo, Y. Deng, B. Li, C. Zhao, and A. Nallanathan, "Eavesdropper localization in random walk channels," *IEEE Communications Letters*, vol. 20, no. 9, pp. 1776–1779, 2016.

[189] K. Yang, D. Bi, Y. Deng, R. Zhang, M. M. U. Rahman, N. A. Ali, M. A. Imran, J. M. Jornet, Q. H. Abbasi, and A. Alomainy, "A comprehensive survey on hybrid communication

in context of molecular communication and terahertz communication for body-centric nanonetworks," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 2, pp. 107–133, 2020.

[190] L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: Body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications*, vol. 31, no. 9, pp. 1803–1816, 2013.

[191] M. M. U. Rahman, Q. H. Abbasi, N. Chopra, K. Qaraqe, and A. Alomainy, "Physical layer authentication in nano networks at terahertz frequencies for biomedical applications," *IEEE Access*, vol. 5, pp. 7808–7815, 2017.

[192] C. Sreeja, M. Misbahuddin, and M. H. NP, "Dna for information security: A survey on dna computing and a pseudo dna method based on central dogma of molecular biology," in *International Conference on Computing and Communication Technologies*. IEEE, 2014, pp. 1–6.

[193] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in dna microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.

[194] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with dna binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, 2000.

[195] A. Gehani, T. LaBean, and J. Reif, "Dna-based cryptography," in *Aspects of Molecular Computing*. Springer, 2003, pp. 167–188.

[196] M. Borda and O. Tornea, "Dna secret writing techniques," in *2010 8th International Conference on Communications*. IEEE, 2010, pp. 451–456.

[197] T. Bakhshi and S. Shahid, "Securing internet of bio-nano things: Ml-enabled parameter profiling of bio-cyber interfaces," in *2019 22nd International Multitopic Conference (INMIC)*. IEEE, 2019, pp. 1–8.

[198] L. Chouhan, P. K. Sharma, P. K. Upadhyay, P. Garg, and N. Varshney, "Impacts of unintended nanomachine in diffusion-based molecular communication system," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 3, pp. 210–219, 2020.

[199] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6913–6924, 2016.

[200] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[201] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[202] Y. Chen and N. C. Beaulieu, "A simple polynomial approximation to the gaussian q-function and its application," *IEEE Communications Letters*, vol. 13, no. 2, pp. 124–126, February 2009.

[203] X. Huang, Y. Fang, A. Noel, and N. Yang, "Channel characterization for 1-d molecular communication with two absorbing receivers," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1150–1154, 2020.

[204] L. Lin, C. Yang, M. Ma, S. Ma, and H. Yan, "A clock synchronization method for molecular nanomachines in bionanosensor networks," *IEEE Sensors Journal*, vol. 16, no. 19, pp. 7194–7203, 2016.

[205] T. Nakano, Y. Okaie, and J. Liu, "Channel model and capacity analysis of molecular communication with brownian motion," *IEEE Communications Letters*, vol. 16, no. 6, pp. 797–800, 2012.

[206] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. US Government printing office, 1964, vol. 55.

[207] J. Lopez-Fernandez and F. J. Lopez-Martinez, "New results on the second order scattering fading model: Amount of fading and energy detection," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 1037–1040, 2020.

List of publications

Journals

Published/Accepted

1. G. Sharma and A. Singh, "Secrecy performance of diffusion based molecular timing channels ", *IET Communications*, vol. 15, no. 2, pp. 289-304, Jan 2021.

2. G. Sharma, N. Pandey, A. Singh and R. K. Mallik, "Secrecy Optimization for Diffusion-Based Molecular Timing Channels", in *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, doi: 10.1109/TMBMC.2021.3054907.

Under Review

1. G. Sharma and A. Singh, "Secrecy Loss in Diffusive Molecular Timing Channels ", *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*.

2. G. Sharma, N. Pandey, A. Singh and R. K. Mallik, "Security in Diffusive Molecular Timing Channels: An Amount of Confusion Level Perspective ", *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*.

Conferences

1. G. Sharma and A. Singh, "On the Optimal Threshold for Diffusion Based Molecular Communication System ", *2018 2nd European Conference on Electrical Engineering and Computer Science (EECS)*, December 2018, pp. 366-370, doi: 10.1109/EECS.2018.00074.

2. G. Sharma and A. Singh, “On the Distribution of Molecules for Diffusion Based Molecular Communication System”, *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, July 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944756.

3. G. Sharma and A. Singh, “On the Optimal Threshold and Error Performance at Fusion Center for Diffusion-Based Molecular Communication System”, *2021 International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, December 2021, (Accepted).