Exploring Security Measures in Molecular Communication

Philip Oguchi and Hakim Lado

School of Computing, University of Nebraska–Lincoln, USA
Email: {eoguchi2,hlado2}@huskers.unl.edu

***Abstract*—The developing field of molecular communication is revolutionizing intercellular communication by using molecules as information carriers. It functions at the nanoscale and microscale levels, providing new opportunities for nanotechnology, biotechnology, and medicine applications. There are many similarities between electromagnetic-based communication and molecular communication. This work provides a thorough comparison and essential distinctions and similarities between electromagnetic and molecular communication regarding their channel capacity, mutual information, secrecy capability, modulation methods, memory and memoryless channels, and security.**

Despite the growing scale of molecular communication, security is in its nascent stage. Our study is part of our course project for the Digital Communication System (CSCE 892). This work contributes to security in the field of molecular and nano communication by simulating a molecular-based scenario involving a transmitter (Alice), a receiver (Bob), and a rogue adversary (Eve). We demonstrate error correction and detection in a molecular diffusive channel by assessing secrecy capacity, channel capacity, and mutual information. Our findings show a secrecy capacity of 2.354, verifying secure communication between Alice and Bob. Bob can also rectify inaccuracies in information molecules (IMs) generated by an advanced attacker. Our findings illustrate that confidentiality and integrity can be maintained even in the presence of passive and active attackers, resulting in trustworthy and secure communication between biological transmitters and receivers.

***Index Terms*—Channel capacity, secrecy capacity, mutual information, Blahut-Arimoto algorithm**

I. Introduction

Molecular communication (MC) is a rapidly developing field that will transform how cells communicate. In recent years, researchers and industry practitioners have explored novel communication paradigms that can enable communication at the microscale and nanoscale levels, where molecules are utilized as information carriers [1]–[4]. Unlike the traditional electromagnetic (EM) based communication systems [5], [6], MC systems can exchange molecules with each other through mediums such as biological fluids, air, and water. While EM communication technologies have long dominated the macroscopic landscape, molecular communication offers a paradigm shift by harnessing the microscopic realm of individual molecules as information carriers. Understanding the intricate relationship between molecular and EM communications becomes paramount for unlocking synergies and addressing emerging security challenges as we navigate this frontier. Despite their apparent dichotomy, these communication paradigms intersect at the nexus of information theory, channel capacity, and security protocols, underscoring their complementary roles in the modern communication ecosystem [7] [3].

The biological cell uses signaling molecules to communicate with each other. Molecular communication draws inspiration from biology and can find its applications in nanotechnology, biotechnology, and medicine. One benefit of molecular communication over traditional electromagnetic communication is that it can operate where EM-based communication faces challenges, like water [8], environmental monitoring [9], and the human body [10]. This makes it possible for drug delivery and biosensing applications [10]–[12] to operate at the microscale, nanoscale, and macroscale distances. This paper compares molecular communication with electromagnetic communication in terms of channel capacity, mutual information, and secrecy capacity.

Molecular communication opens up several security challenges, and the results can be catastrophic. Ensuring the confidentiality, integrity, and availability of transmitted data in molecular communication channels presents unique challenges and opportunities, from mitigating signal interference and molecular noise to safeguarding against eavesdropping and tampering. Robust security measures are essential for fostering trust and reliability in molecular communication infrastructures [3] [11] [13]. Security in molecular communication is still in the nascent stage. As the field of molecular communication evolves, several researchers are increasingly exploring security aspects [14]–[16].

Traditional EM communication systems are fairly more developed than molecular communication as we have several data protection algorithms and systems that guarantee integrity [17], authentication [18], privacy [19], and confidentiality [20]. This security system can not be introduced directly to molecular communication systems [1]. There is a need to develop bio-inspired security systems that can work efficiently with biological systems. Some of the challenges of building such security protocols and systems are the limited computational capability, differences in the channel, modulation/propagation techniques, and the dynamic nature of the molecular environment. Factors such as diffusion rate, molecular interactions, and environmental conditions can influence security reliability in molecular communication.

Molecular-based systems are vulnerable to threats like

eavesdropping, denial of service, spoofing, and jamming attacks. Addressing eavesdropping attacks can help ensure the reliability of information molecules (IMs) transmitted by a biological cell or material. During the exchange of information molecules between cells or communication between two or more nanomachines, noise from that channel can lead to bits flipping or IM degradation as molecules move through the channel, resulting in erroneous data decoded at the receiver. This bit flips, or IM degradation can result from an attack or the channel noise. This paper explores how to guarantee secure and reliable communication between a biological transmitter and a receiver. We make a step to optimize the transmitter to transmit information molecules at an optimized level. The transmitter can use knowledge of the channel to optimize the information molecules being transmitted to increase its channel capacity.

Main Contributions: We present a bio-inspired security measure that shows the relationship with the EM communication paradigm, optimizes the transmitter input distribution using knowledge about the channel, and improves the mutual information, channel capacity, and channel matrix. Our system also solves the problem of information molecules flipping or degradation due to noise from the channel or an advanced adversary attack. We conduct our simulation using defined parameters for the diffusive molecular channel matrix and input distribution. Our evaluation proves that a transmitter can reliably and securely communicate with a receiver in the presence of a passive and an active attacker. We make the following contributions:

- We present a comprehensive system model for molecular communication via diffusion, including an eavesdropper (Eve). The model considers key parameters such as distance, release rate, and environmental conditions, which influence the reception probability and bit error rates at both the legitimate receiver (Bob) and eavesdropper locations.
- We investigate the optimization of the transmitter techniques to transfer information molecules at an optimum level. Using the knowledge about the channel, transmitters can optimize the delivery of information molecules, increasing the channel capacity and ensuring secure and dependable communication between biological transmitters and receivers.
- We describe Eve's interception and disruption capabilities, highlighting the importance of effective communication strategies for risk mitigation. By examining the Eavesdropping attack and bit-flipping attack. We demonstrate the significant effect of eavesdroppers on the communication process and underscore the critical need for advanced security measures in molecular communication systems.
- Finally, we demonstrate an error detection and correction technique due to bit flipping due to a noisy channel or an advanced adversary Eve within the communication range of Alice and Bob. We also compute the secrecy capacity of the system to guarantee that Alice's communication with Bob is secure and reliable.

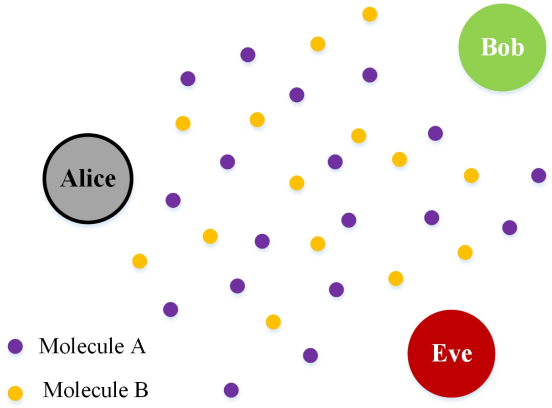

Fig. 1: System Model

Paper Organization: The remainder of the paper is organized as follows: The relationships between Molecular and EM-based Communications are presented in Section II. The System Model and Preliminaries are described in Section III. The Related Work is discussed in Section IV. The Simulation Evaluation is presented in Section V. The Simulation Results are shown in Section VI. The Discussions is presented in Section VII. The paper is concluded in Section VIII.

II. Relationship Between Molecular and Digital Communications

Molecular and Electromagnetic communications deal with transmitting and receiving information via various routes. While EM-based communication can send bits as messages via wave-modulated analog or digital signals through a wired or wireless channel, molecular communication uses information molecules to carry the encoded data between the transmitter and the receiver via a biological or chemical medium. Molecular and EM communications work on different scales, with molecular communications typically occurring at the microscopic level, using individual molecules as information carriers and different modulation techniques [21] like concentration modulation [22], [23], type modulation [24], and timing modulation [25], [26], and EM communications operating at the macroscopic level, using electromagnetic waves for transmission with modulation such as amplitude modulation (AM) [27], frequency modulation (FM) [28] and phase modulation (PSK) [29] [30]. The modulation techniques in molecular communication are based on the properties of the diffusion and reaction in the medium, while EM-based modulation techniques are based on manipulating the properties of electromagnetic waves and the electrical properties at the macroscopic level.

The channel properties in molecular communications are influenced by factors like diffusion rate, molecule degradation, distance, and environmental conditions, while EM communication channel properties are influenced by factors such as bandwidth, noise, path loss, attenuation, signal-to-noise

ratio, and multipath propagation properties [31]. These properties will influence the evaluation using metrics like mutual information, channel capacity, secrecy capacity, [32], [33], which are important for analyzing both EM-based systems and molecular-based systems. We compare these evaluation metrics for both EM-based systems and molecular-based systems.

A. Channel Capacity

In EM communications, channel capacity refers to the maximum rate at which information may be reliably carried over a communication channel. This is frequently influenced by bandwidth, noise, and power limitations [34]. Contrastingly, in MC, channel capacity refers to the maximum rate at which information may be reliably communicated using information molecules as carriers. The capacity is determined by molecular diffusion rate, signaling molecule concentration, distance, and environmental circumstances [35]. MC and EM channels share a similar concept of channel capacity, but they differ significantly in the factors that influence this channel capacity.

Unlike EM channels, which can exhibit memoryless and memory characteristics, most practical MC channels have memory, which introduces additional complexity compared to traditional EM channels. This is due to the nature of molecular interactions and diffusive processes. A substance's diffusion rate through another is described by Fick's law of diffusion [36]. It is frequently employed in many disciplines, including engineering, biology, physics, and chemistry. Understanding processes like the diffusion of gases, fluid, or tissue across membranes, the spread of environmental pollutants, or the diffusion of drugs through biological tissues is made easier with the help of Fick's law [37]. It helps to model the diffusion of signaling molecules across the communication medium. Researchers can acquire larger channel capacities in molecular communication systems by optimizing their design with an awareness of these concepts. Controlling variables, including the rate at which signaling molecules are released, the characteristics of the communication channel, and the sensing and detection systems that interpret the communicated data, may all be part of this optimization process.

Past transmission influences future receptions, leading to dependencies between consecutive transmissions and receptions. In this case, channel capacity is calculated differently [38]. A memory-based system implies that it can lead to inter-symbol interference (ISI), where one symbol's reception affects subsequent symbols' reception, leading to errors in decoding transmitted information. The combination of molecular diffusion, absorption, and reception probability can cause variations in reception quality over time, affecting the overall reliability of the communication link. Memoryless channels operate standalone, meaning past transmission does not influence future reception. This means modulation and demodulation processes in EM-based systems are straightforward, reducing ISI and error correction burden.

The channel capacity C for a EM communication system [39] where $I(X;Y)$ is the mutual information between a transmitted signal X and a received signal Y given as

$$C = \max_{f_X(x)} I(X;Y) \tag{1}$$

Therefore, channel capacity can then be represented in terms of the entropy where $H(X)$ is the input entropy and $H(X/Y)$ is the entropy of X conditioned on signal Y given as

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

The channel capacity C for a diffusive based MC system as defined in [40], [41] for Alice-to-Bob (C_{AB}) and Alice-to-Eve (C_{AE}) is given as

$$\begin{aligned}
C_{\text{AB}} &= 2W_{AB}\left(1+\log_2\frac{P_{H_{AB}}}{3W_{AB}K_{b_{AB}}T_{AB}}\right) \\
&\quad -\log_2\left[(\pi d_{AB}D_{AB})^2\right] - \frac{4d_{AB}}{3\ln 2}\sqrt{\frac{\pi W_{AB}}{D_{AB}}} \\
&\quad -2W_{AB}\eta_{AB} - 2W_{AB}\ln\left(W_{AB}\frac{r_{R_{AB}}^2}{D_{AB}}\right) \\
&\quad -2W_{AB}\ln(\Gamma(\eta_{AB})) - 2W_{AB}(1-\eta)\Psi(n_{AB}), \\
C_{\text{AE}} &= 2W_{AE}\left(1+\log_2\frac{P_{H_{AE}}}{3W_{AE}K_{b_{AE}}T_{AE}}\right) \\
&\quad -\log_2\left[(\pi d_{AE}D_{AE})^2\right] - \frac{4d_{AE}}{3\ln 2}\sqrt{\frac{\pi W_{AE}}{D_{AE}}} \\
&\quad -2W_{AE}\eta_{AE} - 2W_{AE}\ln\left(W_{AE}\frac{r_{R_{AE}}^2}{D_{AE}}\right) \\
&\quad -2W_{AE}\ln(\Gamma(\eta_{AE})) - 2W_{AE}(1-\eta)\Psi(n_{AE})
\end{aligned} \tag{3}$$

Where P_{H_X} is the signaling molecule concentration between entities X, W_X is the channel bandwidth, K_{b_X} is the Boltzmann's constant, D_X is the diffusion coefficient, d_X is the distance, $r_{R_X}^2$ is the radius of the receiver effective absorbing area, and n_X is the number of absorbed molecules between entities X.

B. Mutual Information

In an EM-based system, mutual information is the amount of information that one random variable (in this case, the transmitted signal) has about another random variable (the received signal). Mutual information in EM communications measures how much information is consistently communicated via a channel, taking into account noise and other limitations [34]. Mutual information functions similarly in molecular communications by quantifying information flow between the transmitter (source of signaling molecules) and the receiver. It shows how much information is successfully communicated despite the unpredictable nature of molecule diffusion [35]. This concept is critical in understanding and optimizing communication systems where signals are transmitted via molecular or chemical means. Channel memory and molecular noise are vital in quantifying mutual information for an MC-based system.

In traditionally EM-based systems, the mutual information $I(X;Y)$ between X and Y reduces uncertainty about signal Y

due to the knowledge of signal X, and vice versa is expressed as:

$$I(X;Y) = H(Y) - H(Y|X), \tag{4}$$

Equation (4) can be expressed in terms of their probabilities [34] from the Bayes rule as

$$I(X;Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \tag{5}$$

Similarly, the channel capacity for MC systems, bio-inspired mutual information as defined in [41] in terms of Alice-to-Bob and Alice-to-Eve is expressed as:

$$\begin{aligned} I(X;Y)_{\text{AB}} &= 2W_{AB}H(\overrightarrow{n}_{Tx})_{AB} - \log_2\left[(\pi d_{AB}D_{AB})^2\right] \\ &\quad -\frac{4d_{AB}}{3\ln 2}\sqrt{\frac{\pi W_{AB}}{D_{AB}}} - 2W_{AB}\eta \\ &\quad -2W_{AB}\ln(W_{AB}\tau_p) - 2W_{AB}\ln(\Gamma(\eta)) \\ &\quad -2W_{AB}(1-\eta)\Psi(n_{AB}), \\ I(X;Y)_{\text{AE}} &= 2W_{AE}H(\overrightarrow{n}_{Tx})_{AE} - \log_2\left[(\pi d_{AE}D_{AE})^2\right] \\ &\quad -\frac{4d_{AE}}{3\ln 2}\sqrt{\frac{\pi W_{AE}}{D_{AE}}} - 2W_{AE}\eta \\ &\quad -2W_{AE}\ln(W_{AE}\tau_p) - 2W_{AE}\ln(\Gamma(\eta)) \\ &\quad -2W_{AE}(1-\eta)\Psi(n_{AE}). \end{aligned} \tag{6}$$

Where $\overrightarrow{n}_{Tx_X}$ is the discrete-time of the particle concentration between entities X, W_X is the channel bandwidth, D_X is the diffusion coefficient, d_X is the distance, τ_p is the time interval of the constant particle distribution, which depends on how far the particle can escape the receiver, $\Gamma(\cdot)$ and $\Psi(\cdot)$ are the gamma function and the digamma function, and n_X is the number of absorbed molecules between entities X.

C. Secrecy Capacity

Secrecy capacity (C_s) is the greatest rate at which information can be securely transferred via a communication channel while preventing unauthorized parties from intercepting and deciphering the transmission. Encryption algorithms [42], [43] and secure key exchange mechanisms accomplish secrecy in EM-based communications. Because of the specific properties of molecular communication pathways, obtaining secrecy capacity requires similar concepts but differing implementation methodologies. To ensure that the appropriate recipient only receives the message approaches such as chemical camouflage or the use of particular receptors on receiver cells can be utilized [35]. The secrecy capacity for an EM-based system for the communication of Alice and Bob in the presence of Eve is mathematically modeled as:

$$C_s = \max_{P_{X|Y}} I(X;Y) - \max_{P_{X|Z}} I(X;Z). \tag{7}$$

where $I(X;Y)$ is the mutual information between the transmitted signal X and the received signal at Bob Y, $I(X;Z)$ is the mutual information between the transmitted signal X and the received signal at Eve Z. $P_{X|Y}$ and $P_{X|Z}$ are the conditional probability distributions of X given Y and Z respectively. Secrecy capacity can also be represented in terms of their channel capacity [35] as:

$$C_s = \max\{C_{AB} - C_{AE},\ 0\}. \tag{8}$$

III. System Model and Preliminaries

The system model shown in Fig.1 comprises three nanomachines: a point transmitter, Alice, a legitimate absorbing receiver, Bob, and an absorbing eavesdropper, Eve.

Alice and Bob communicate by releasing information molecules (IMs), which then spread throughout the system. The communication channels include various elements such as reception probabilities, diffusion rates, release rates, distance, and environmental variables. These elements influence the dependability and security of communication. Alice is transmitting IM to Bob in the presence of Eve in the system. In this system, we assume that the distance d between Alice and Bob is invariant, but we can still vary it during the evaluation of the channel capacity with respect to the distance, R_d the rate of diffusion, P_i the reception probability, R_i the release rate of the i^{th} information molecule IM. The system is based on the following assumptions:

- The diffusion-based MC channel extends infinitely in all three spatial dimensions (x, y, z), and the transmitter releases identical molecules that cannot be differentiated. These molecules can be conceptualized as spherical particles with a specific radius r and mass m.
- The transmitter is a point located at the coordinates $(0, 0, 0)$. Each molecule, upon emission, moves autonomously from the others and follows its own Brownian motion. The movement of a molecule in Brownian motion is a stochastic process described by the Langevin equation [44].
- The valid receiver detects a signal directly proportional to the concentration of the entering particles.

A. Modulation and Transmission Model

We consider a Discrete Memoryless Channel (DMC) system utilizing D-MoSK modulation [35], [45]. Alice can release N different kinds of IMs. At the commencement of a time slot, Alice transmits a symbol x represented by m binary bits, with each bit denoted as a single kind of IM: $x = (x^{(1)}, x^{(2)}, \ldots, x^{(m)})$. We denote $Q^{(i)}$ as the number of released IMs of the i^{th} type, for $i = 1, 2, \ldots, m$. The i^{th} bit of x, or $x^{(i)}$, is set to $''1''$ if Alice releases $Q^{(i)}$ IMs; otherwise, it is set to "$0''$. Hence, in general, Alice can send 2^m different symbols by regulating the emission of various IM types [21], [35]. In this particular simulation work, Alice released only 2 types of IMs, as shown in Fig. 1

B. Probability of Reception of Molecules by Bob and Eve Model

The probability of reception in molecular communication is contingent upon multiple factors, including the propagation method, environmental conditions, and receiver characteristics.

Understanding and modeling these probabilities is crucial for designing efficient and reliable molecular communication systems. The probability of reception can be modeled as follows:

1) Basic Diffusion Model: A basic model to estimate the probability that a molecule released by Alice reaches Bob through diffusion in a 3D space is given:

$$P_{\text{receive}} = \frac{r}{d} \exp\left(-\frac{d^2}{4Dt}\right), \tag{9}$$

where r is the radius of Bob's effective absorbing area, d is the distance between Alice and Bob, D is the diffusion coefficient, t is the time post-release.

2) Improved Model: For environments involving flow or reactive conditions, the reception model is adjusted. If there is a flow towards Bob, the probability of reception P_{receive} is given as

$$P_{\text{receive}}(d, u) = \frac{r}{d} \exp\left(-\frac{(d-ut)^2}{4Dt}\right), \tag{10}$$

where u is the flow velocity towards the receiver, and t is the time post-release, which is the time elapsed since the molecules were released by Alice. In an environment where molecules may degrade over time, the probability of reception is modified as

$$P_{\text{receive}} = \frac{r}{d} \exp\left(-\frac{d^2}{4Dt} - \lambda t\right). \tag{11}$$

Where λ is the molecular degradation rate.

3) Probability of Bit Error: The probability that Bob correctly decodes a bit depends on P_{receive} and the detection threshold δ. This detection probability is modeled using the Poisson distribution:

$$P(\text{bit error}) = P(M < \delta | \text{bit} = 1) + P(M \geq \delta | \text{bit} = 0)$$

Where M is the number of detected molecules. Each term can be expressed as:

$$P(M < \delta | \text{bit} = 1) = e^{-\lambda_1 t} \sum_{k=0}^{\eta-1} \frac{(\lambda_1 t)^k}{k!}, \tag{12}$$

$$P(M \geq \delta | \text{bit} = 0) = 1 - e^{-\lambda_0 t} \sum_{k=0}^{\eta-1} \frac{(\lambda_0 t)^k}{k!}. \tag{13}$$

λ_1 and λ_0 are the average numbers of molecules received corresponding to bits '"1" and "0", respectively.

C. Decoding Model

Since the absorption processes of distinct types of IMs are independent of one another [45]–[48], each binary bit in a symbol can be decoded individually by comparing the number of absorbed IMs corresponding to this bit to the set threshold for this bit [49]. To establish the decoding rule for a symbol x with m binary bits in a D-MoSK system, use the decoding rule for the one-bit symbol in a BCSK-based system [2].

The decoding rule is given as follows:

$$x = \begin{cases} 00\ldots0, & \text{if } \lambda(n) > \lambda(1), \lambda(2), \ldots, n_b^{(m)} \\ 00\ldots1, & \text{if } n_b^{(1)} < \lambda(1), \lambda(2), \ldots, n_b^{(m)} \geq \lambda(n) \\ \vdots & \vdots \\ 11\ldots1, & \text{if } \lambda(n) \geq \lambda(1), \lambda(2), \ldots, n_b^{(m)} \end{cases}$$

Where $n_b^{(i)}$ represents the total number of the i-th ($i = 1, 2, \ldots, m$) kind of IMs absorbed by Bob in a given time slot, and $\lambda(i)$ represents the threshold for the i-th type of IM. If $n_b^{(i)}$ is more than or equal to $\lambda(i)$, the i-th bit of symbol x ($x(i)$) is set to "1", otherwise it is set to "0".

D. Threat Model

We present an eavesdropper, Eve, as illustrated in Fig. 1. Eve is an absorbing adversary within the communication range of Alice and Bob, who has the capability to

- listen, intercept, and absorb the IM intended for Bob.
- Eve also has an advanced capability that releases IM that flips the content of the IM intended for Bob.

Eve achieves this by positioning herself within Alice and Bob's communication range since the MC system is not confined to physical boundaries. Eve can position herself to eavesdrop on messages intended for Bob. Eve can potentially intercept the molecules as they diffuse through the medium. Eve attempts to decode the information molecules, flip the content, and forward the message to Bob. Eve can also emit/ release molecules that can increase the concentration of the channel or cause interference by releasing IM to flip the content of the IM sent to Bob. These can impede Bob's ability to effectively decipher his messages or cause him to misunderstand the communication and decode error-prune IM.

IV. Related Work

The challenges of molecular in nano-network communication security are investigated [50], noting the shortcomings of traditional methods. Bio-inspired cryptography is suggested as a potential solution, alongside discussions on system vulnerabilities and the importance of robustness. The authors discussed the various communication techniques, and their security implications are explored. Jia *et al.* [35], analyze the secrecy performance of the 3-D diffusive molecular communication system. They derive probabilistic distributions for the molecules absorbed by both Bob and Eve, considering IMs released by Alice, ISI molecules, and noisy molecules. The authors evaluated the average symbol error rate (SER), the mutual information of Alice-Bob and Alice-Eve, and information leakage. Understanding these metrics is crucial for optimizing system parameters, enhancing communication efficiency, and designing secure protocols to ensure reliable and confidential communication. Pierobon *et al.* and Mucchi *et al.* also derive the channel capacity, secrecy capacity, mutual information, and information leakage for a diffusive base molecular communication system. They also introduce the concept of secured distance for the MC system within which

the communication is termed secured. They also discussed channel memory and noise in MC systems.

The critical need to address security and privacy concerns in MC systems due to their unique characteristics is emphasized by Loscri *et al.* [51]. The existing cryptographic methods are deemed inadequate for MC networks, necessitating tailored solutions to safeguard information transmission. Many authors [4], [50]–[53] highlight the challenges and open issues related to security in MC, underscoring the urgency of developing effective defense mechanisms. By drawing inspiration from biological systems, such as the immune system, researchers can explore innovative approaches to enhance security in MC networks. Overall, they stressed the importance of interdisciplinary collaboration and novel bio-inspired techniques to ensure the security and privacy of molecular communication. Although the authors [3], [14], [52], [54] are trying to address the security of the MC system, many of these works focus on passive attackers, where an absorbing eavesdropper within the communication range of the transmitter and receiver tries to leak information and cause harm.

Very few works address active attacks in MC-based systems [55]–[57]. Shahbaz *et al.* studies jamming attacks in MC systems, in which the jammer tries to disrupt the information from reaching the receiver. They proposed a jamming-resistant coding scheme to counteract this attack. They assumed that the jammer releases an equal number of molecules at the beginning of the subplots, which is a difficult assumption to make in real-life scenarios. Martins *et al.* also studied jamming attacks to suppress bacterial biofilm formation. They used staphylococcus aureus biofilm formation as a communications system and showed how it can be engineered to prompt and suppress biofilm-related proteins. The authors took a more practical approach to show the actual suppression of IM in bacteria from the receiver bacterial cell.

Many researchers [15], [35], [41], [58], [59] have worked on security in molecular-based systems from an information theory perspective, but they have not discussed how the transmitter can optimize its input transmission using knowledge about the channel. Our paper introduces a way for the transmitter to optimize the input distribution of its IM using knowledge about the channel. We also optimize the channel matrix to improve the channel capacity, mutual information, and secrecy capacity in an MC-based system in the presence of an absorbing eavesdropper.

Despite the progress recorded in security in molecular and nano-based communication, there are still a plethora of security challenges. These challenges include message integrity, confidentiality, authentication, and availability in molecular-based systems. This motivated us to investigate message integrity and confidentiality in molecular-based systems. We leverage the error detection and correction technique used in EM-based systems to develop a molecular-inspired error correction and detection that corrects the bit flipped due to an attacker or noise in the channel at the receiver. Our approach guarantees that more secured IM will be received at the receiver reliably and ensures integrity by correcting errors in the IM due to an adversary or noise in the channel

Algorithm 1 Blahut-Arimoto Algorithm

Input: Transition matrix $q(y|x)$, optimize $p_i(x)$, $p_i(y|x)$
Output: Capacity C
Initialize $p^{(0)}(x)$ arbitrarily such that $\sum_x p^{(0)}(x) = 1$
$n \leftarrow 0$
repeat
  Compute $p(y) \leftarrow \sum_x p^{(n)}(x)p(y|x)$
  for each x **do**
    Compute $q(x) \leftarrow \exp\left(\sum_y p(y|x) \log \frac{p(y|x)}{p(y)}\right)$
  end for
  Compute normalization factor $Z \leftarrow \sum_x p^{(n)}(x)q(x)$
  Update $p^{(n+1)}(x) \leftarrow \frac{p^{(n)}(x)q(x)}{Z}$
  $n \leftarrow n + 1$
until convergence criteria met ($|I^{(n)} - I^{(n-1)}| < \epsilon$)
$C \leftarrow \sum_{x,y} p^{(n)}(x)p(y|x) \log \frac{p(y|x)}{p(y)}$ ▷ Compute the channel capacity
return C, $p^{(n)}(x)$

V. Simulation Evaluation

We conduct an experimental analysis of our work, describing our simulation setup and simulation results to show that our work is correct and robust. Our simulation setting utilizes the Blahut-Arimoto algorithm to calculate the secrecy capacity between Alice and Bob and between Alice and Eve. This algorithm optimizes input distributions, representing the probability of transmitted molecules, to calculate channel capacity.

Simulation Setup: Our setup simulates a molecular communication scenario between Alice and Bob over a noisy channel. Eve, an eavesdropper, may intercept and temper the message. We define two communication channel matrices, one between Alice and Bob and the other between Alice and Eve. The channel matrix probabilities are adjusted based on the release rate, distance, and environmental conditions. This adjustment simulates real-world conditions that may affect the reliability and security of communication. We set Alice's original input distribution as [0.5, 0.5]. We set the parameters for transmission, such as the release rate of 1.5 symbols per second, distance of 2.0 meters, and environmental conditions at 1.2 decibels per meter. The environmental conditions affect Alice's transmission, including the interference level, signal-to-ratio, and error rate.

We also define the channel matrix for Alice-to-Bob and Alice-to-Eve. The channel capacity is calculated for both Alice-to-Bob and Alice-to-Eve communication channels using the Blahut-Arimoto algorithm. This algorithm optimizes the input distribution of signaling molecules to maximize the channel capacity. We define and compute the mutual information to measure the amount of information shared between Alice and Bob and between Alice and Eve based on the optimized input distributions and conditional probabilities. We compute the secrecy capacity between Alice and Bob in the

presence of Eve to measure the maximum rate at which Alice then transmits information molecules to Bob. This will ensure that Alice and Bob's communication is kept confidential from Eve.

Eve intercepts and tampers with the message, which is then forwarded to Bob. Bob verifies the integrity of the received message by checking for errors and correcting them. The parameters and values for our experimental setup and simulation results are shown in Table I and II.

VI. Simulation Results

Algorithm 2 Secrecy Capacity Maximization

Input: Transition matrix $Q(y|x)$
Output: Secrecy Capacity C_s
Initialize p_i, release rate r_i , receiver distance d_i, channel matrix Q_i, input symbols s_i
repeat
  $Q_i^{'} \leftarrow$ AdjustMatrix(Q_i)
  $p_i(x) \leftarrow$ OptimizeInput($Q_i^{'}, r_i, d_i$)
  $p_i(y|x) \leftarrow$ ComputePmartix($Q_i^{'}, p_i(x)$)
  $C_i \leftarrow$ BlahutArimoto($q(y|x), p_i(x), p_i(y|x)$)
  $C_{si} \leftarrow$ SecrecyCapacity($q(y|x), p_i(x), p_i(y|x)$)
until $s_i = 0$
return C_s

TABLE I: Channel Parameters and Capacity (Alice to Bob)

Parameter	Value
Original Channel Matrix	$\begin{bmatrix} 0.4 & 0.1 \\ 0.6 & 0.4 \end{bmatrix}$
Adjusted Channel Matrix	$\begin{bmatrix} 0.36 & 0.09 \\ 0.54 & 0.36 \end{bmatrix}$
Optimized Input Distribution	$[0.3566, 0.6434]$
Probability $P(Y\|X)$	$[0.6434, 0.3566]$
Channel Capacity	0.6301

TABLE II: Channel Parameters and Capacity (Alice to Eve)

Parameter	Value
Original Channel Matrix	$\begin{bmatrix} 0.2 & 0.05 \\ 0.3 & 0.2 \end{bmatrix}$
Adjusted Channel Matrix	$\begin{bmatrix} 0.18 & 0.045 \\ 0.27 & 0.18 \end{bmatrix}$
Optimized Input Distribution	$[0.3566, 0.6434]$
Probability $P(Y\|X)$	$[0.6434, 0.3566]$
Channel Capacity	-0.3599

TABLE III: Message Integrity Check

Parameter	Value
Original Message from Alice	$[1, 0, 1, 1]$
Encoded Message from Alice to Bob	$[1, 0, 1, 1, 0, 1, 0]$
Eve Flipped Bit at Index	6
Decoded Message at Bob	$[1, 0, 1, 1]$

TABLE IV: Simulation Results

Parameter	Alice to Bob	Alice to Eve
Channel Capacity	0.630	-0.360
Mutual Information	0.940	0.940
Secrecy Capacity	2.354	

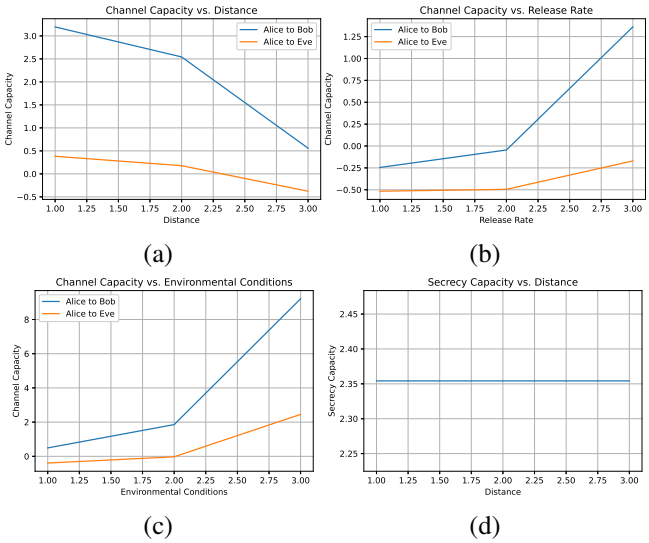

Fig. 2: Plots of the optimized channel capacity for Alice-to-Bob and Alice-to-Eve while varying (a) the distance, (b) The release rate, (c) the environmental conditions, (d) Plots of the secrecy capacity of the system against the distance.

A. Legitimate Channel (Alice to Bob)

We compute that the legitimate optimized channel capacity from Alice to Bob was calculated to be 0.630 using the adjusted input by using Algorithm 1, representing the highest possible rate of reliable information transmission. In Fig. 2 (a), (b), (c), we show that the channel capacity varies with respect to distance, release rate, and environmental conditions. From Fig. 2 (a), the channel capacity degrades with an increase in distance for both the channel from Alice and Bob and Alice to Eve, which means that for optimum communication, the distance between Alice and Bob is an important factor to consider. We observe from Fig. 2 (b) and (c) that channel capacity improves as the release rate and environment condition increases. Using Algorithm 2, we computed the secrecy capacity at which Alice can securely communicate information to Bob in the presence of Eve, which was determined to be 2.354. The positive value indicates that Alice can transmit IM securely to Bob without Eve being able to decode it.

Furthermore, we computed the mutual information between Alice and Bob to be 0.940 with the optimized input distribution after applying Algorithm 1, representing the average amount of information Alice can send to Bob with each symbol. However, an advanced adversary defined in Section III that intercepts the IM from Alice to Bob and tampers with it will be detected by Bob and corrected, indicating message integrity guarantees. Our simulation results are shown in Table IV.

B. Eavesdropped Channel (Alice to Eve)

In the eavesdropped channel scenario, Alice communicates with Eve rather than Bob; the channel capacity was determined

to be -0.360 as shown in Fig. IV, showing that Alice can not reliably transmit meaningful information molecules to Eve due to interference in the channel from Alice since the adjusted channel matrix from Alice to Bob is mainly different from Alice to Eve.

It is clear from comparing the findings of the legitimate and eavesdropped channels that the existence of an eavesdropper greatly reduces the feasible transmission rate by altering the channel capacity. Nonetheless, the capacity for secrecy is preserved, meaning Alice can safely converse with Bob even when Eve is around. Alice can communicate securely with Bob in the presence of Eve, and in the worst case, advanced adversary, Bob can correct IM that was intercepted and tampered with by Eve.

VII. Discussions

A. Analysis of Simulation Results

The simulation outcomes demonstrate how resilient the communication system is in maintaining secure communication between Alice and Bob in case of an eavesdropper. While the secrecy capacity study quantifies the rate at which sensitive information can be conveyed, the channel capacity analysis shows the highest possible transmission rate that can be achieved. Optimizing the channel capacity means Alice can reliably send more IMs to Eve. The analysis of optimized mutual information sheds light on how much information is exchanged between Alice and Bob. From our result, Alice can exchange more IMs with Bob. The error correction and detection show that if Eve intercepts and tampers with the IM, Bob can still decode the information accurately by correcting the error. This guarantees message integrity in our system, as shown in Fig. III. Our error correction techniques are defined in such a way that it is lightweight and computationally less expensive and can work with Molecular and nano-base scenario.

B. Performance of the System

The system successfully achieves secure communication between Alice and Bob by maintaining a high level of secrecy despite eavesdropping attempts. Although the channel capacity is reduced in the presence of an eavesdropper, the transmission is still safe, ensuring that Alice's information is not intercepted by Eve. Eavesdropping significantly impacts the channel capacity, lowering the possible transmission rate. The system's ability to maintain secrets is unchanged, demonstrating resistance to eavesdropping attempts. According to the investigation, even when eavesdropping efforts are made, the system can preserve secure communication and guarantee integrity. We perform this experiment in various settings of distance, release rate, and environment and show how the channel capacity of our system varies with respect to changes in these settings. We show in Fig. 2 (a), (b), and (c) that the channel capacity is highly affected by changes in the distance, the release rate of the IM, and the environmental conditions. Alice-to-Eve shows better channel capacity due to our optimized input distribution from the channel. Fig. 2 (d) also shows that secrecy capacity remains stable while the distance changes from [1-3]m.

VIII. Conclusion

In conclusion, our simulation study shows how the communication system works to achieve secure communication between Alice and Bob in the presence of an eavesdropper, Eve, for an MC-based system. Despite the reduced channel capacity, the system retains a high level of secrecy, guaranteeing that Alice's information is protected. While the investigation of secrecy and channel capacity emphasizes the system's resistance to eavesdropping attacks, the inclusion of error detection and correction techniques improves message integrity.

While the system demonstrates promising capabilities, continuous research and development are required to address growing security concerns and improve communication security. To guarantee that secure communication systems remain effective, future work should focus on enhancing encryption algorithms, adapting to dynamic contexts, and raising user awareness. Future research proposals include investigating new security measures and enhancing the system's resilience to more advanced eavesdroppers and active attacker.

References

[1] L. Chouhan and M.-S. Alouini, "Interfacing of molecular communication system with various communication systems over internet of every nano things," *IEEE Internet of Things Journal*, 2023.

[2] 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.

[3] 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.

[4] T. Nakano, M. J. Moore, F. Wei, A. V. Vasilakos, and J. Shuai, "Molecular communication and networking: Opportunities and challenges," *IEEE transactions on nanobioscience*, vol. 11, no. 2, pp. 135–148, 2012.

[5] Y. A. Sambo, F. Heliot, and M. A. Imran, "A survey and tutorial of electromagnetic radiation and reduction in mobile communication systems," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 790–802, 2014.

[6] J. V. Stone, "Information theory: a tutorial introduction," 2015.

[7] 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.

[8] Y. Huang, W. Gan, X. Chen, D. Tang, J. Li, and M. Wen, "An energy-efficient ternary modulation with water for molecular communication systems: From solvent to information carrier," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2024.

[9] Z. Sakkaff, A. Freiburger, N. Gupta, M. Pierobon, and C. S. Henry, "Information-and communication-centric approach in cell metabolism for analyzing behavior of microbial communities," *bioRxiv*, pp. 2023–08, 2023.

[10] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 58–63, 2010.

[11] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The internet of bio-nano things," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 32–40, 2015.

[12] N. Ntetsikas, S. Kyriakoudi, A. Kirmizis, B. D. Unluturk, A. Pitsillides, I. F. Akyildiz, and M. Lestas, "Engineering yeast cells to facilitate information exchange," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2024.

[13] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of nano things: Security issues and applications," in *Proceedings of the 2018 2nd international conference on cloud and big data computing*, 2018, pp. 71–77.

[14] Y. Huang, M. Wen, L. Lin, B. Li, Z. Wei, D. Tang, J. Li, W. Duan, and W. Guo, "Physical-layer counterattack strategies for the internet of bio-nano things with molecular communication," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 82–87, 2023.

[15] G. Sharma, R. K. Mallik, N. Pandey, and A. Singh, "Effect of interfering transmitter on the secrecy of diffusive molecular timing channels," *IEEE Transactions on Communications*, 2024.

[16] G. Sharma, N. Pandey, A. Singh, and R. K. Mallik, "Impact of mutual influence between bob and eve on the secrecy of diffusion-based molecular timing channels," *IEEE Wireless Communications Letters*, vol. 11, no. 11, pp. 2255–2259, 2022.

[17] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, M. A. Towfiq, and B. A. Cetiner, "Message integrity protection over wireless channel: Countering signal cancellation via channel randomization," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 106–120, 2017.

[18] M. Cagalj, S. Capkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava, and J.-P. Hubaux, "Integrity (i) codes: Message integrity protection and authentication over insecure channels," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, 2006, pp. 15–pp.

[19] 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.

[20] W. Lou, W. Liu, and Y. Fang, "Spread: Enhancing data confidentiality in mobile ad hoc networks," in *IEEE INFOCOM 2004*, vol. 4. IEEE, 2004, pp. 2404–2413.

[21] 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)*. IEEE, 2011, pp. 1–5.

[22] 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.

[23] W.-A. Lin, Y.-C. Lee, P.-C. Yeh, and C.-h. Lee, "Signal detection and ISI cancellation for quantity-based amplitude modulation in diffusion-based molecular communications," in *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 4362–4367.

[24] G. Aminian, M. Mirmohseni, M. N. Kenari, and F. Fekri, "On the capacity of level and type modulations in molecular communication with ligand receptors," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 1951–1955.

[25] M. U. Mahfuz, D. Makrakis, and H. Mouftah, "Spatiotemporal distribution and modulation schemes for concentration-encoded medium-to-long range molecular communication," in *2010 25th Biennial Symposium on Communications*. IEEE, 2010, pp. 100–105.

[26] H. B. Yilmaz and C.-B. Chae, "Simulation study of molecular communication systems with an absorbing receiver: Modulation and isi mitigation techniques," *Simulation Modelling Practice and Theory*, vol. 49, pp. 136–150, 2014.

[27] Y. Sato, "A method of self-recovering equalization for multilevel amplitude-modulation systems," *IEEE Transactions on communications*, vol. 23, no. 6, pp. 679–682, 1975.

[28] B. Van Der Pol, "Frequency modulation," *Proceedings of the Institute of Radio Engineers*, vol. 18, no. 7, pp. 1194–1205, 1930.

[29] J. B. Anderson, T. Aulin, and C.-E. Sundberg, *Digital phase modulation*. Springer Science & Business Media, 2013.

[30] H. Roder, "Amplitude, phase, and frequency modulation," *Proceedings of the Institute of Radio Engineers*, vol. 19, no. 12, pp. 2145–2176, 1931.

[31] H. Zhang, T. Zhou, T. Xu, M. Cheng, and H. Hu, "Field measurement and channel modeling around wailingding island for maritime wireless communication," *IEEE Antennas and Wireless Propagation Letters*, 2024.

[32] 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.

[33] J. Zhu, Z. Wan, L. Dai, M. Debbah, and H. V. Poor, "Electromagnetic information theory: Fundamentals, modeling, applications, and open problems," *IEEE Wireless Communications*, 2024.

[34] P. Hwei P. HSU, *Theory and Problems of Analog and Digital Communications*. The McGraw-Hill, 2003.

[35] Z. Jia, L. Ma, S. Shen, and X. Jiang, "On Secrecy Performance in D-MoSK-based 3-D Diffusive Molecular Communication System," *IEEE Transactions on NanoBioscience*, 2023.

[36] D. Jaynes and A. Rogowski, "Applicability of fick's law to gas diffusion," *Soil Science Society of America Journal*, vol. 47, no. 3, pp. 425–430, 1983.

[37] S. M. Mustam, S. K. Syed-Yusof, and S. Zubair, "Capacity and delay spread in multilayer diffusion-based molecular communication (dbmc) channel," *IEEE transactions on nanobioscience*, vol. 15, no. 7, pp. 599–612, 2016.

[38] R. G. Gallager, *Information theory and reliable communication*. Springer, 1968, vol. 588.

[39] T. M. Cover, *Elements of information theory*. John Wiley & Sons, 1999.

[40] 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.

[41] M. Pierobon and I. F. Akyildiz, "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.

[42] C. Gentry, *A fully homomorphic encryption scheme*. Stanford university, 2009.

[43] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, 2022, pp. 365–390.

[44] G. E. Uhlenbeck and L. S. Ornstein, "On the theory of the brownian motion," *Physical review*, vol. 36, no. 5, p. 823, 1930.

[45] J. Wang, X. Liu, M. Peng, and M. Daneshmand, "Performance analysis of d-mosk modulation in mobile diffusive-drift molecular communications," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11 318–11 326, 2020.

[46] M. H. Kabir, S. R. Islam, and K. S. Kwak, "D-mosk modulation in molecular communications," *IEEE transactions on nanobioscience*, vol. 14, no. 6, pp. 680–683, 2015.

[47] J. Wang, M. Peng, and Y. Liu, "Performance analysis of diffusion-based decode-and-forward relay with depleted molecule shift keying," *Digital Communications and Networks*, vol. 7, no. 3, pp. 399–409, 2021.

[48] M. S. Thakur, S. Sharma, and V. Bhatia, "Iterative signal detection to mitigate isi and mui for diffusion-based molecular communications," *Nano Communication Networks*, vol. 30, p. 100377, 2021.

[49] X. Chen, Y. Huang, L.-L. Yang, and M. Wen, "Generalized molecular-shift keying (gmosk): Principles and performance analysis," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 3, pp. 168–183, 2020.

[50] F. Dressler and F. Kargl, "Security in nano communication: Challenges and open research issues," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 6183–6187.

[51] 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.

[52] J. Andréasson and U. Pischel, "Molecules for security measures: from keypad locks to advanced communication protocols," *Chemical Society Reviews*, vol. 47, no. 7, pp. 2266–2279, 2018.

[53] S. P. Singh, S. Yadav, and S. Mishra, "Secrecy capacity of diffusive molecular communication under biological spherical environment," in *Proceedings of the 1st ACM International Workshop on Nanoscale Computing, Communication, and Applications*, 2020, pp. 33–38.

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

[55] D. P. Martins, K. Leetanasaksakul, M. T. Barros, A. Thamchaipenet, W. Donnelly, and S. Balasubramaniam, "Molecular communications pulse-based jamming model for bacterial biofilm suppression," *IEEE transactions on nanobioscience*, vol. 17, no. 4, pp. 533–542, 2018.

[56] D. P. Martins, M. T. Barros, and S. Balasubramaniam, "Using competing bacterial communication to disassemble biofilms," in *Proceedings of the 3rd ACM International Conference on Nanoscale Computing and Communication*, 2016, pp. 1–6.

[57] S. Shahbaz, M. Mirmohseni, and M. Nasiri-Kenari, "A jamming resistant molecular communication scheme," in *2022 10th Iran Workshop on Communication and Information Theory (IWCIT)*. IEEE, 2022, pp. 1–6.

[58] G. Sharma, N. Pandey, A. Singh, and R. K. Mallik, "Secrecy optimization for diffusion-based molecular timing channels," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 7, no. 4, pp. 253–261, 2021.

[59] L. Mucchi, A. Martinelli, S. Caputo, S. Jayousi, and M. Pierobon, "Secrecy capacity of diffusion-based molecular communication systems," in *13th EAI International Conference on Body Area Networks 13*. Springer, 2020, pp. 103–114.