Secrecy Performance of Molecular Communication with an Absorbing Eavesdropper and D-MoSK Modulation

Zhen JIA[†a)], **Lisheng MA**[††], **Shigen SHEN**[†††], ***and*** **Xiaohong JIANG**[†],

SUMMARY Secure information transmission of molecular communication (MC) systems is an important research aspect. This paper investigates the maximum achievable secrecy rate in a diffusion-based molecular communication system with the depleted molecule shift keying (D-MoSK), a legitimate absorbing receiver and an eavesdropper. We first calculate the mutual information of the legitimate link, and then obtain the maximum achievable rates for the legitimate link and the information leakage by maximizing the mutual information. Based on the maximum achievable rate and information leakage, we further derive the maximum achievable secrecy rate. Finally, we evaluate and discuss the impacts of critical parameters on the maximum achievable secrecy rate. The results in this paper are helpful for the design of MC systems with high achievable secrecy rate.
key words: *Molecular communication, D-MoSK modulation, Secrecy rate*

1. Introduction

With the development of nanotechnology, the Internet of Bio-Nano Things (IoBNT) has been proposed to realize the practical application of bio-embedded devices [1]. IoBNTs have a wide range of potential applications, such as disease treatment, health monitoring and drug delivery [2]. Generally, IoBNTs are used in microscale scenarios, such as living organisms, which cannot be satisfied by conventional electromagnetic communication techniques. Since molecular communication (MC) can use molecules to communicate at the microscale, it is considered as one of the promising ways to realize IoBNT.

In MC, molecular communication via diffusion (MCvD) is the most widely way to exchange information between nanomachines. In an MCvD system, a transmitter first modulates the information based on the molecule concentration (BCSK), molecule releasing time (TM) and molecule type (D-MoSK) [3]. Then the molecules are released and diffuse randomly in the environment. A receiver detects or absorbs molecules and decodes the information. Since an absorbing receiver can reuse molecules to save limited resources, in this paper, we focus on an MCvD system with an absorbing receiver.

Information security has always been an important issue of communication systems, especially in an MC system where health-related information is transmitted. In the studies of secure transmission of MC system, the authors in [4] obtained a closed expression of the secrecy capacity from a thermodynamic point of view. Considering a timing channel using OOK modulation, the authors in [5] gave closed-form expressions for the eavesdropping capacity and generalized security outage probability. Based on [5], the generalized secrecy outage probability was minimized in [6]. The above studies consider MC systems with monitoring receivers where the eavesdropper does not affect the legitimate link. However, in practical scenarios, an MC system with absorbing receivers is also considered. In such a system, an eavesdropper absorbs the information molecules, resulting in fewer molecules absorbed by the legitimate receiver. On the other hand, the secrecy rate is an important index to reflect the information that can be securely transmitted. Thus, in [7], considering an MCvD system with an absorbing receiver and an absorbing eavesdropper, the secrecy rate based on BCSK modulation was first studied. Compared with BCSK, D-MoSK has lower complexity and higher data rate, which has been studied in various MC systems [3][8]. Unfortunately, the research on the secrecy rate of the MCvD system with D-MoSK modulation and absorbing receiver is still an open issue, which poses a potential threat to the practical application of D-MoSK. Thus, in this paper, we study the maximum achievable secrecy rate (MASR) of an MCvD system with a legitimate absorbing receiver and an absorbing eavesdropper where D-MoSK modulation is adopted.

To achieve the MASR of the MCvD system, we first use poisson distribution to obtain the number of molecules received by the legitimate receiver. After that, the maximum achievable rate is formulated by maximizing the mutual information. Based on these, the information leakage and maximum achievable secrecy rate are derived. Finally, the impacts of system parameters on the MASR are evaluated. Numerical results show that the locations of the eavesdropper have obvious effects on the MASR. Our work can provide guidelines to improve the maximum achievable secrecy rate.

The remainder of this paper is organized as follows: the system model for the MCvD system is presented in Section 2. The MASR of this system with D-MoSK modulation is presented in Section 3. Numerical results are presented in Section 4. Finally, Section 5 gives the conclusions.

2. System model

In this section, an MCvD system is considered with a point transmitter Alice, an absorbing legitimate receiver Bob with radius of a_1 and an absorbing eavesdropper Eve with radius of a_2. These nanomachines are fixed in an unbounded 3D environment, as showed in Fig. 1. In this system, Alice is

[†]The author is with the Future University Hakodate, Hakodate, Japan.
[††]The author is with the Chuzhou University, Anhui, China.
[†††]The author is with Huzhou University, Huzhou, China.
a) E-mail: jiazhen@snnu.edu.cn

located at point x (0, 0, 0), denoted as origin of 3D coordinate system. Bob and Eve are located at points x_1 and x_2, respectively. The distances from Alice to Bob and Alice to Eve are r_1 and r_2, respectively. Here, ϕ is the angle between vector $\overrightarrow{xx_1}$ and $\overrightarrow{xx_2}$.

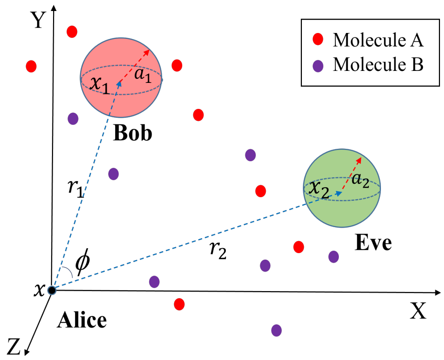

Fig. 1 A 3D MCvD system with a point transmitter Alice, an absorbing legitimate receiver Bob and an absorbing eavesdropper Eve.

Consider that the communication time is divided into time slots with equal length T_s. At the beginning of the j_{th} T_s, Alice releases molecules into the environment according to the D-MoSK modulation. Here, Alice utilizes two types of molecules (type A or type B) to represent first or second bits of symbol S_γ ($\gamma \in \{0, 1, 2, 3\}$). If the symbol $S_0 = (0, 0)$ is transmitted, Alice does not release any molecule. When Alice only releases the molecule A or molecule B, the transmitted symbol is $S_1 = (1, 0)$ or $S_2 = (0, 1)$, respectively. When Alice releases both type A and type B molecules, the transmitted symbol is $S_3 = (1, 1)$.

We define $p(t, k_d)$ as the probability that a molecule is released from Alice and reaches to Bob in time t with the presence of Eve. The approximate expression of $p(t, k_d)$ can be denoted as [9]

$$\mathrm{p}(t, k_d) = \sum_{k=0}^{\infty} \left(\frac{a_1 a_2}{R_{12} R_{21}} \right)^k \left[\frac{a_1}{r_1} f\left(\Phi_1(k)\right) - \frac{a_1 a_2}{r_2 R_{21}} f\left(\Psi_1(k)\right) \right] \tag{1}$$

where $R_{12} = \sqrt{(r_1 - a)^2 + r_2^2 - 2(r_1 - a) \cdot r_2 \cos(\phi)}$, $R_{21} = \sqrt{(r_2 - a)^2 + r_1^2 - 2(r_2 - a) \cdot r_1 \cos(\phi)}$ and k is a natural number. We set $\Phi_1(k) = r_1 - a_1 + k(R_{21} - a_1) + k(R_{12} - a_2)$ and $\Psi_1(k) = r_2 - a_2 + (k + 1)(R_{21} - a_1) + k(R_{12} - a_2)$. The function $f(\chi)$ in (1) is defined as $f(\chi) = \frac{1}{2} \operatorname{erfc}\left(\frac{\chi}{\sqrt{4Dt}} + \sqrt{k_d t} \right) \exp\left(\chi \sqrt{\frac{k_d}{D}} \right) + \frac{1}{2} \operatorname{erfc}\left(\frac{\chi}{\sqrt{4Dt}} - \sqrt{k_d t} \right) \exp\left(-\chi \sqrt{\frac{k_d}{D}} \right)$, where D is the diffusion coefficient, $\operatorname{erfc}(\cdot)$ is the complementary error function and k_d denotes the degradation reaction constant.

For absorbing molecules and decoding the information of Bob, the specific detection rule can be written as

$$Y[j] = \begin{cases} 00, \text{ if } N_t^A[j] < \eta^A, N_t^B[j] < \eta^B, \\ 10, \text{ if } N_t^A[j] \geq \eta^A, N_t^B[j] < \eta^B, \\ 01, \text{ if } N_t^A[j] < \eta^A, N_t^B[j] \geq \eta^B, \\ 11, \text{ if } N_t^A[j] \geq \eta^A, N_t^B[j] \geq \eta^B, \end{cases} \tag{2}$$

where $Y[j]$ represents the detected symbol at Bob in time slot j. $N_t^A[j]$ and $N_t^B[j]$ are the total number of type A and type B molecules received in the j_{th} slot, respectively. η^A and η^B are the decision thresholds of the j_{th} symbol. When $N_t^\mu[j] \geq \eta^\mu[j]$ ($\mu \in \{A, B\}$), the bit corresponding to molecule μ in the j_{th} symbol will be decoded as "1", otherwise "0".

3. Secrecy Rate Analysis

In this section, we firstly calculate the number of molecules absorbed by Bob. Then the maximum achievable rate of Bob and information leakage is derived. Finally, the maximum achievable secrecy rate is derived by calculating the difference between the maximum achievable rate and the information leakage.

3.1 Mutual Information and Maximum Achievable Rate

At the beginning of the j_{th} time slot, Alice releases type A and type B molecules to transmit four kinds of symbols. Then the number of type μ ($\mu \in \{A, B\}$) molecules absorbed by Bob at j_{th} time slot $N_t^\mu[j]$ can be expressed by

$$N_t^\mu[j] = N_c^\mu[j] + N_p^\mu[j] + N_n^\mu[j], \tag{3}$$

where $N_c^\mu[j]$ is the number of type A or B molecules released at the beginning of the j_{th} slot and absorbed by the receiver within the j_{th} slot. $N_p^\mu[j]$ refers to the molecules released in the previous slots but reaches to receiver at the j_{th} slot, i.e., inter-symbol interference (ISI). $N_n^\mu[j]$ is the number of noisy molecules.

For a large number of molecules and small arrival probability, $N_c^\mu[j]$ can be approximated by poisson distribution as [7]

$$N_c^\mu[j] \sim \mathcal{P}\left(x^\mu[j] M^\mu p_0\right), \tag{4}$$

where $p_0 = p(T_s, k_d)$, $x^\mu[j] \in \{0, 1\}$ denotes the transmitted bit corresponding to type A or type B molecules of the j_{th} symbol, and M^μ represents the number of released molecules when the input bit is "1". Then ISI $N_p^\mu[j]$ can be given as

$$N_p^\mu[j] \sim \sum_{l=1}^{L} \mathcal{P}\left(x^\mu[j - l] M^\mu p_l\right), \tag{5}$$

where L stands for the length of ISI and $p_l = p((l + 1)T_s, k_d) - p(lT_s, k_d)$ denotes the probability that a molecule is emitted at the previous l time slot but absorbed by the receiver in the j_{th} time slot.

According to the properties of poisson distribution, we define $\lambda_1 = \sum_{l=0}^{L} x^\mu[j - l] M^\mu p_l + \lambda_n$ and $\lambda_0 = \sum_{l=1}^{L} x^\mu[j - l] M^\mu p_l + \lambda_n$ to represent the average number of molecules received when bit "1" and bit "0" are transmitted, respectively. λ_n is the average number of noise molecules $N_n^{\mu}[j]$ [9]. Therefore, the transition probability of a bit in the j_{th} symbol can be written as

$$\begin{aligned}
\Pr\left(y^{\mu}[j]=1 \mid x^{\mu}[j]=1\right) &= 1-\sum_{i=1}^{\lfloor \eta^{\mu} \rfloor} \frac{e^{-\lambda_1[j]}\cdot(\lambda_1[j])^i}{i!},\\
\Pr\left(y^{\mu}[j]=0 \mid x^{\mu}[j]=1\right) &= \sum_{i=1}^{\lfloor \eta^{\mu} \rfloor} \frac{e^{-\lambda_1[j]}\cdot(\lambda_1[j])^i}{i!},\\
\Pr\left(y^{\mu}[j]=0 \mid x^{\mu}[j]=0\right) &= \sum_{i=1}^{\lfloor \eta^{\mu} \rfloor} \frac{e^{-\lambda_0[j]}\cdot(\lambda_0[j])^i}{i!},\\
\Pr\left(y^{\mu}[j]=1 \mid x^{\mu}[j]=0\right) &= 1-\sum_{i=1}^{\lfloor \eta^{\mu} \rfloor} \frac{e^{-\lambda_0[j]}\cdot(\lambda_0[j])^i}{i!},
\end{aligned} \tag{6}$$

where $y^{\mu}[j]$ denotes the detected bit corresponding to type A or type B molecules in the j_{th} time slot.

Based on the above equation, the transition probability of a symbol S_{γ} ($\gamma \in \{0,1,2,3\}$) can be obtained as

$$\begin{aligned}
P(S_0 \mid S_0) &= \Pr\left(y^A[j]=0 \mid x^A[j]=0\right)\\
&\quad \times \Pr\left(y^B[j]=0 \mid x^B[j]=0\right),\\
P(S_1 \mid S_0) &= \Pr\left(y^A[j]=1 \mid x^A[j]=0\right)\\
&\quad \times \Pr\left(y^B[j]=0 \mid x^B[j]=0\right),\\
P(S_2 \mid S_0) &= \Pr\left(y^A[j]=0 \mid x^A[j]=0\right)\\
&\quad \times \Pr\left(y^B[j]=1 \mid x^B[j]=0\right),\\
P(S_3 \mid S_0) &= \Pr\left(y^A[j]=1 \mid x^A[j]=0\right)\\
&\quad \times \Pr\left(y^B[j]=1 \mid x^B[j]=0\right).
\end{aligned} \tag{7}$$

The transition probability for S_1, S_2 and S_3 can be obtained in a similar way.

Assuming that all symbols are transmitted with equal probability, we can get $P(S_{\gamma}) = \frac{1}{4}$, $\gamma \in \{0,1,2,3\}$. Then the mutual information of the j_{th} symbol can be given as

$$\begin{aligned}
&I(X[j];Y[j])\\
&= \sum_{Y[j]\in\{S_{\gamma}\}} \sum_{X[j]\in\{S_{\gamma}\}} P(S_{\gamma})P(Y[j]|X[j])\\
&\times \log_2 \frac{P(Y[j]|X[j])}{\sum\limits_{X[j]\in\{S_{\gamma}\}} P(S_{\gamma})P(Y[j]|X[j])} \quad \text{bits/slot.}
\end{aligned} \tag{8}$$

where $X[j]$ and $Y[j]$ are the transmitted and decoded symbol at Bob in j_{th} time slot.

We assume that the molecule A and B have the same diffusion coefficient D and $M^A = M^B = M$. Then the η^{μ} can be written as η_b as the threshold for Bob. Thus, the maximum achievable rate is given by

$$C_b = \max_{\eta_b} I(X[j];Y[j]) \quad \text{bits/slot.} \tag{9}$$

3.2 Maximum Achievable Secrecy Rate

According to the mutual information of the legitimate channel, we can similarly obtain the information eavesdropped by Eve. We treat the amount of information that Eve stole as information leakage [4]. Let $Z[j]$ denotes the decoded symbol at Eve in j_{th} time slot, the information leakage can be written as

$$\begin{aligned}
&I(X[j];Z[j])\\
&= \sum_{Z[j]\in\{S_{\gamma}\}} \sum_{X[j]\in\{S_{\gamma}\}} P(S_{\gamma})P(Z[j]|X[j])\\
&\times \log_2 \frac{P(Z[j]|X[j])}{\sum\limits_{X[j]\in\{S_{\gamma}\}} P(S_{\gamma})P(Z[j]|X[j])} \quad \text{bits/slot.}
\end{aligned} \tag{10}$$

The MASR can be derived as the maximum of the difference between the maximum achievable rate of the legitimate communication link and the information leakage [4], expressed as

$$\begin{aligned}
C_s &= \max(I(X[j];Y[j]) - I(X[j];Z[j]))\\
&\geq \max_{\eta_b}(I(X[j];Y[j])) - \max_{\eta_e}(I(X[j];Z[j]))\\
&= C_b - C_e \quad \text{bits/slot,}
\end{aligned} \tag{11}$$

where η_e is the threshold of Eve, C_b and C_e can be determined by changing η_b and η_e, respectively [10]. Since the secrecy rate cannot be negative, the MASR can be written as

$$C_s \geq \{C_b - C_e, 0\} \quad \text{bits/slot.} \tag{12}$$

4. Numerical Results and Discussions

In this section, the maximum achievable secrecy rate (MASR) for the MCvD system with an absorbing legitimate receiver Bob and an absorbing eavesdropper Eve is analyzed. The impacts of several important parameters such as the distance between Alice and Eve, time slot duration and diffusion coefficient on the MASR are investigated. Here, we set $a_1 = a_2 = 1\times10^{-6}$m, $k_d = 0.1$/s, $M = 10^3$, $\lambda_n = 20$, $L = 10$. Here, $x_1 = (20\times10^{-6}, 0, 0)$, $x_2 = (0, \Gamma\times10^{-6}, 0)$ ($\Gamma \in \{22, 24, 26\}$), thus, $r_1 = 20\times10^{-6}$m, $r_2 = \Gamma\times10^{-6}$m, and $\phi = \frac{\pi}{2}$.

Firstly, the MASR is obtained for different time slot duration T_s, where r_2 is considered as 22×10^{-6}m, 24×10^{-6}m, 26×10^{-6}m, respectively. We assume that the diffusion coefficient D is set as 10×10^{-11} m^2/s. From the results in Fig.2, we find that MASR first increases and then decreases with the increase of T_s. This is because when T_s increases, both Bob and Eve absorb more information molecules, increasing the maximum achievable rate and the information leakage. Since $r_1 < r_2$ and the hit probability of a molecule $p(t, k_d)$ decreases with the increase of distance, Bob absorbs more molecules than Eve. As a result, the increase of the maximum achievable rate of Bob is higher than the increase of information leakage, leading to the MASR increases. When T_s continues to increase (e,g., $r_2 = 22$um, $T_s > 2$s), the number

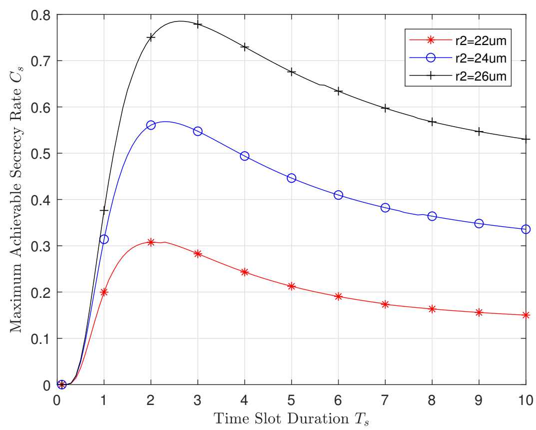

Fig. 2 The MASR obtained for different time slot duration T_s.

of molecules absorbed by Eve increases and the information leakage increases, leading to the decrease of MASR. It can be seen in Fig.2 that the MASR increases as r_2 increases. The reason is that a larger r_2 indicates a lower probability of absorbing molecules, leading to lower information leakage and higher MASR.

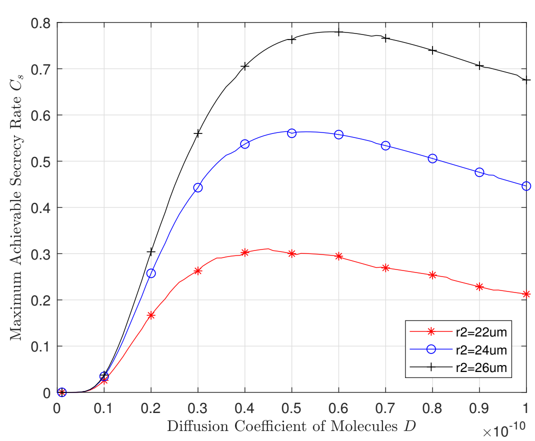

Fig. 3 The MASR obtained for different diffusion coefficient D.

The MASR is then shown for the different diffusion coefficients of molecules D in Fig.3, where different distances r_2 are considered, and T_s is fixed as 5s. For the same value of D, it can be seen that the MASR increases as r_2 increases, which is similar to that in Fig.2. It can then be observed that the MASR first increases and then decreases as D increases. The result can be explained as follows. The increase of D represents the increase of the diffusion speed of the molecules. When D increases from small to large, more information molecules can reach Bob within T_s. Thus, the maximum achievable rate of Bob increases faster than information leakage and the MASR increases. Due to the random movement of molecules, a larger diffusion coefficient D (e.g., $r_2 = 26um$, $D > 0.6 \times 10^{-10}$) will increase the uncertainty of molecular movement. Therefore, the number of molecules absorbed by Bob decreases, and the MASR decreases.

5. Conclusion

This paper investigated an MCvD system with a legitimate absorbing receiver and an absorbing eavesdropper. We applied the D-MoSK modulation to this concerned system and analyzed the secrecy performance. By jointly considering the ISI effect and the noise, the maximum achievable rate, information leakage and maximum achievable secrecy rate (MASR) are derived. The numerical results show that the MASR is highly related to the location of the eavesdropper. The obtained results are expected to be helpful for the design of MCvD systems with high secrecy rate requirement.

Acknowledgment

This work was supported by the Key Project of Chuzhou University Science Research (No.2022XJZD11).

References

[1] 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.

[2] L. Huang, W. Wang, S. Shen, "Energy-efficient coding for electromagnetic nanonetworks in the Terahertz band," *Ad Hoc Networks*, vol. 40, pp. 15-25, 2016.

[3] Z. Cheng, J. Yan, Y. Tu, K. Chi and M. Xia, "Mobile Two-Way Molecular Communication via Diffusion Using Amplify-and-Forward and Analog Network Coding," *IEEE Transactions on NanoBioscience*, vol. 21, no. 2, pp. 273-285, 2022.

[4] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo and M. Pierobon, "Secrecy Capacity and Secure Distance for Diffusion-Based Molecular Communication Systems," *IEEE Access*, vol. 7, pp. 110687-110697, 2019.

[5] G. Sharma, A. Singh, "Secrecy Performance of Diffusion based Molecular Timing Channels," *IET Communications*, vol. 15, pp. 289-304, 2021.

[6] 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.

[7] 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.

[8] 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. 11318-11326, 2020.

[9] N. V. Sabu, N. Varshney and A. K. Gupta, "On the Performance of the Primary and Secondary Links in a 3-D Underlay Cognitive Molecular Communication," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8028-8041, 2021.

[10] J. Zhu, Y. Chen and M. Sasaki, "Average Secrecy Capacity of Free-space Optical Communication Systems with On-off Keying Modulation and Threshold Detection," *2016 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 616-620, 2016.