IEEE Internet of Things Magazine, Volume 6, Issue 2, June 2023, pp. 82-87
DOI: 10.1109/IOTM.001.2300029

Physical-layer Counterattack Strategies for the Internet of Bio-Nano things with Molecular Communication

Yu Huang, Miaowen Wen, Lin Lin, Bin Li, Zhuangkun Wei, Dong Tang, Jun Li, Wei Duan, and Weisi Guo

***Abstract*—Molecular communication (MC) is an emerging new communication paradigm where information is conveyed by chemical signals. It has been recognized as one of the most promising physical layer techniques for the future Internet of Bio-Nano Things (IoBNT), which enables revolutionary applications beyond our imagination. Compared with conventional communication systems, MC typically demands a higher security level as the IoBNT is deeply associated with the biochemical process. Against this background, this article first discusses the security and privacy issues of IoBNT with MC. Then, the physical-layer countermeasures against the threat are presented from an interdisciplinary perspective concerning data science, signal processing techniques, and the biochemical properties of MC. Correspondingly, both the keyless and key-based schemes are conceived and revisited. Finally, some open research issues and future research directions for secrecy enhancement in IoBNT with MC are put forward.**

I. Introduction

The past decades have witnessed great achievements in the Internet of Things (IoT). Despite being deployed on the general scale, the IoT is envisioned to be used in the micro-scale scenario when specific applications are required. Thanks to the advancement of nanotechnology, the concept of the Internet of NanoThings (IoNT) is conceived, where nano-scale devices can be connected intelligently. Despite having the potential for revolutionary applications, e.g., nano-scale healthcare systems and targeted drug delivery, the artificial nature of IoNT may bring a latent threat to the health system. Against this background, the Internet of Bio-Nano Things (IoBNT) is further presented as an updated version of the IoNT [1], where the synthetic biology domains are further taken into account, getting rid of the side effect of the IoNT. While 5G lacks the capability to support the IoBNT, 6G is envisioned to tackle this issue by forming heterogeneous networks, which include the nano-/micro-scale network with nano-devices [2]. Inspired by nature, molecular communication (MC), which uses the characteristics of molecules for information exchange, has been recognized as one of the most prominent schemes for IoBNT due to its bio-compatibility, energy efficiency, and prevalence in nature [1].

Compared with the conventional network, the applications in MC networks, such as IoBNT, are usually associated with human health. Thus, a higher security level is required than conventional networks as the loophole can cause catastrophic consequences. To the best of our knowledge, the concept of nano-scale communication security was first proposed in [3], which suggests that traditional cryptography may not be feasible due to the lack of computing power and resource. When MC is deployed in IoBNT, the novel biochemical cryptography that exploits the biological and chemical features is required to improve the system's security in terms of key management, access control, authentication, etc. Following this work, the security and privacy of MC are discussed via a layered perspective (from the physical layer to the application layer) [4]. In addition to the biochemical cryptography [3], other bio-inspired network approaches based on artificial immune systems and swarm intelligence, are regarded as viable solutions to safeguard the nano-/micro-scale MC networks. Moreover, latent bio-terrorism against future healthcare applications (e.g., localization and search of the diseased cells) based on IoBNT with MC was introduced in [5]. Specifically, the blackhole attack distracts the legitimate nodes from reaching their target by emitting chemo-attractants, while the chemo-repellents are used in another attack mechanism, called sentry attack. Concerning the properties of the IoBNT with MC, the authors designed lightweight methods for both attacks.

Over the years, the research of MC mainly focuses on information transmission efficiency, while its security is seldom studied. Motivated by the pioneering works [3]–[5] with regard to the MC security, the existing techniques dissatisfy the trust, secrecy, and privacy demanded by the prospective applications involved with IoBNT. Therefore, it is essential to revisit the achievements, and more importantly, explore novel solutions for the security enhancement of the IoBNT and other MC networks, which is the main contribution of this article. In the rest of this article, we first present the security requirement of the multi-scale MC networks, where the micro-scale scenario is emphasized. Then, we introduce physical layer security (PLS) with both key-based and keyless schemes to safeguard the MC networks. Finally, some open issues regarding the security of the MC networks are discussed, and a conclusion is drawn.

Y. Huang is with Research Center of Intelligent Communication Engineering, School of Electronics and Communication Engineering in Guangzhou University, and also with Guangdong Provincial Key Laboratory of Short-Range Wireless Detection and Communication, School of Electronic and Information Engineering in South China University of Technology. D. Tang, and J. Li are with Research Center of Intelligent Communication Engineering, School of Electronics and Communication Engineering, Guangzhou University. M. Wen is with South China University of Technology. L. Lin is with Tongji University. B. Li is with Beijing University of Posts and Telecommunications. Z. Wei and W. Guo are with Cranfield University. W. Duan is with Nantong University. The corresponding authors are Dong Tang and Jun Li.

This work was supported in part by the National Natural Science Foundation of China under Grant 62201161, in part by the Tertiary Education Scientific research project of Guangzhou Municipal Education Bureau under Grant 202235019, in part by the Guangzhou Science and Technology Project under Grants SL2022A04J01273 and 2023A03J0110, in part by EPSRC CHEDDAR (EP/X040518/1) and EPSRC TAS-S (EP/V026763/1), in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515030118, and in part by Open Funding of Guangdong Provincial Key Laboratory of Short-Range Wireless Detection and Communication.

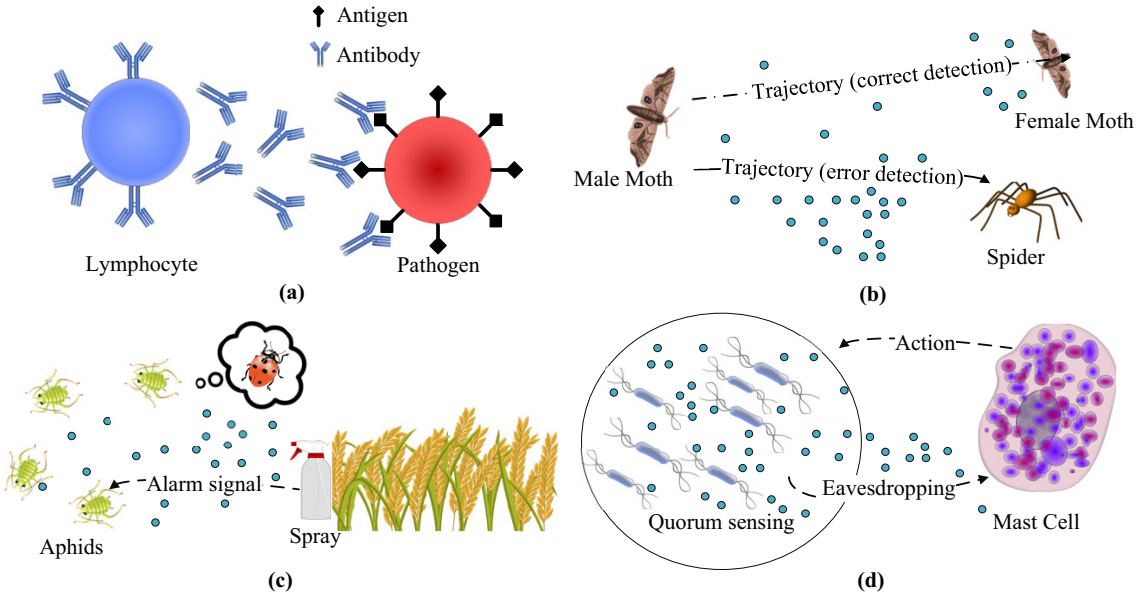

Fig. 1. Natural attack and eavesdropping examples with the MC mechanism.

II. Security Challenges in Molecular Communication Networks

MC encodes its message according to the characteristics of the information molecule, such as concentration level, emission time/space, and molecular type. It has multi-scale deployments, ranging from the micro-scale scenario (e.g., cell signaling, cooperative targeted drug delivery within the IoBNT) to the macro-scale scenarios (e.g., deep ocean long-distance localization, covert messaging for the wave-denied environments). Despite having versatile applications, it faces security challenges like other communication paradigms.

A. Attacks in Molecular Communication

Figure 1 exemplifies the attack and eavesdropping cases in the natural multi-scale MC networks, where the blue circles represent the information molecules in each scenario. Like conventional communication systems, each layer in the MC system encounters its own attacks [4]. As MC is still in its infancy, the research of the physical layer is at the top of the agenda, supporting the success of the higher layers. Attacks in the physical layer include hardware tampering, degradation of information molecules, jamming signals, etc.

Hardware tampering: It is one of the most fundamental attack mechanisms, in which the attackers break the communication devices physically. Here, a corresponding example in nature is the antigen-antibody interaction as Fig. 1(a) shows. To counteract such an attack, identification is the first step that determines the legitimacy of the nodes in the channel, which can be accomplished by the guard devices. Once the unexpected invaders are detected, they are destroyed by the guard devices. Owing to the biochemical nature of the micro-scale MC channel, a swarm of the nano-robots can serve as the guard devices by mimicking the functionality of the biological immune system, recognizing the malicious devices and destroying them.

Consequently, a higher security level can be guaranteed in this context, once the guard devices are self-evolving, behaving like an adaptive immune system. By incorporating data science (training and learning) and proper programming, they can tackle new challenges.

Degradation of information molecules: In MC, the messages are carried via the chemical features of the information molecules. Thus, their degradation deteriorates the quality of service in the MC networks. In this regard, the malicious devices may release the enzymes (e.g., lipase that catalyzes the hydrolysis of lipids), emit light (e.g., ultraviolet light that transforms the pro-vitamin D to pre-vitamin D), modify the local environment parameters (the high temperature that leads to the denaturation of the nucleic acids or protein), etc., to cause degradation or decomposition of the information molecules. As a result, the stability of information molecules is the top priority for the MC system design.

For instance, given the appropriate temperature, the ammonium ion (NH_4^+) is stable in an acidic environment and can be used as the information molecule, while it is unstable in an alkaline environment. Furthermore, one may take advantage of the diversity provided by the ionic compound, which consists of positively and negatively charged ions, i.e., cations and anions, respectively. When sodium chloride (NaCl) is chosen as the information molecule dissolved in the aqueous channel (e.g., water), both the characteristics of sodium ion (Na^+) and chloride (Cl^-) can be used for information decoding. In this case, even if one type of the charged ions is removed from the channel, e.g., the malicious device releases silver ion (Ag^+) into the channel, synthesizing the silver chloride (AgCl) with low solubility, the other still exists, and the decoding process can be accomplished as well. However, the molecular diversity gain of the ionic compound is obtained at the expense of transceiver complexity.

Jamming signal: Malicious devices can severely affect the

performance of MC by introducing jamming signals to disturb the reception of the legitimate receiver, causing error detection or false alarm events. As shown in Fig. 1(b), some spider species emit identical sex pheromones (jamming signal) of female moths, imitating their existence to attract the male moths and prey on them. Hence, novel signal processing techniques are required to counteract such attacks from the PLS perspective, which will be elaborated upon further in the next section. Moreover, Fig. 1(c) demonstrates a pest control strategy that uses the alarm pheromone of the aphid species, mimicking the alarm signal, to expel them and protect plants.

B. Wiretap Channel

Quorum sensing (QS) is the extracellular signaling among bacteria that coordinates gene expressions (e.g., virulence, biofilm formation, antibiotics resistance) via specific QS molecules. As Fig. 1(d) shows, the mast cells are found to use receptors, namely, Mrgprb2 and MRGPRX2, eavesdropping on the QS mechanism. Once the QS molecules are detected, mast cells are activated to secrete tumor necrosis factor, reactive oxygen species, and prostaglandin D_2 to fight against bacteria for sake of the host benefit [6]. In light of this, malicious devices, on the other hand, may act as unintended receivers, obtaining vital information, and posing the threat to MC networks' security and privacy in addition to the aforementioned attacks. Compared with the macro-scale networks, the micro-scale networks bears increased privacy as the eavesdropper has to infiltrate *in vivo*. On the contrary, this indicates that higher security and privacy levels are required as the information being exchanged may contain health conditions or therapeutic plans, whose leakage may lead to a devastating impact. The countermeasures against wiretapping in MC networks include but are not limited to, secure channel establishment, localization of the eavesdropper, and secret transmission strategy.

Secure channel establishment: The random movement of the small particles in the fluid channel is known as the diffusion mechanism, which is prevalent in nature. It is also widely adopted in the MC networks as no external infrastructure or energy is needed during the propagation process of the information molecules. When no boundaries and external factors such as flow and reaction are involved, the spreading of a large amount of the information molecules follows an isotropic manner provided that the channel has a constant diffusion coefficient in all dimensions. Against this background, the free diffusion-based MC channels suffer from the same risk as a conventional wireless channel due to the broadcast nature.

To overcome this problem, one may establish a secure channel by changing the chemical pattern or building a new structure between the legitimate transceivers. For the former case, the legitimate transceiver can achieve the high directivity gain and low leakage of MC by the reflection of the transmitter and prior position alignment [7]. This process is analogous to the beamforming technique of conventional wireless communication systems, and concerning the physics in the MC channel, the assistance of the flow can further enhance the secrecy performance. For the latter case, specific

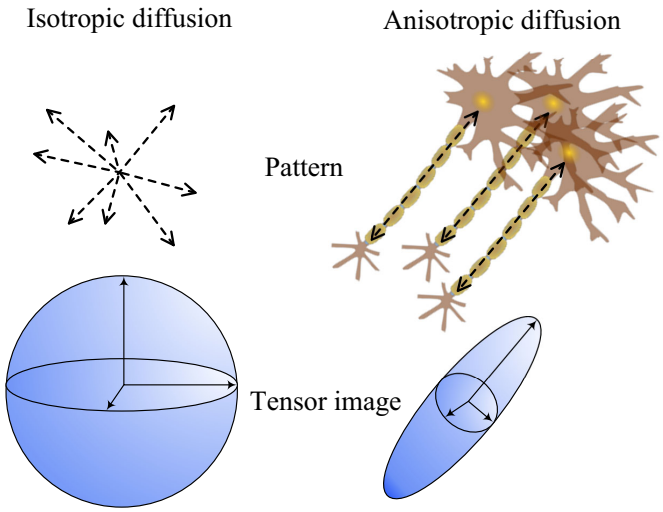

Fig. 2. Comparison of chemical propagation patterns.

structures (e.g., axon) that convert the isotropic diffusion to the anisotropic diffusion can be deployed in the channel, creating a secure channel/zone for information transmission. Figure 2 shows the corresponding diffusion pattern and the tensor image. Intuitively, information disclosure is avoided as the eavesdropper hardly captures the information molecules. Nevertheless, the success of both countermeasures is based on the premise that the position of the eavesdropper (its localization methods are discussed in the next subsection) is not close to the line of sight path between the transceiver or the orientation of the new structure.

Localization of the eavesdropper: Localization not only enables applications like targeted drug delivery, target search and rescue in MC networks, but also reveals the location of the eavesdropper to enhance the secrecy performance. The detection of a silent eavesdropper, which only listens in the channel without information transmission, is an arduous process. In conventional EM-based wiretap channels, the legitimate nodes detect the silent eavesdropper in light of its unintentionally leaked local oscillator power. However, this method may not be available in the MC networks when the biochemical property dominates in the physical layer. Alternatively, silent eavesdroppers in the MC channel may exhibit the absorbing phenomenon during the interception process. Thus, except for the detection of silent entities in MC, its localization can be further realized. So far, MC researchers have proposed the localization schemes of the silent eavesdropper from one-dimensional (1-D) to three-dimensional (3-D) channels.

The authors in [8] first considered this issue based on a simple end-to-end system model with a point transmitter and two perfectly absorbing receivers. Note that the 1-D channel model applies to scenarios where the length dimension dominates, while the height and width dimensions are negligible, such as blood vessels, pipes, and tubes. In particular, detection and localization of the silent eavesdropper are conducted by the transmitter only as information transmission in the MC system is typically unidirectional, and feedback from the receiver may not be possible. Thereafter, the transmitter is

further equipped with optical detectors, acting as a passive receiver to count the information molecules released by itself. With prior knowledge of the legitimate transceiver distance, the eavesdropper's location can be easily estimated via the reduction of the information molecules.

The issue above can be extended to the two-dimensional (2-D) MC scenarios, where the flat petri dish is one of the examples of the bounded channel. An unbounded 2-D channel with a point transmitter and two circular receivers that are perfectly absorbing is considered in [9]. The legitimate receiver, instead of the transmitter, is used to detect and localize the eavesdropper. Since the channel modeling of multiple absorbing MC receivers is still under exploration, no analytical arrival distribution at the receivers is available. Motivated by the data-driven approach, a deep neural network is trained via the data generated from the particle-based simulator. It then employs the received signal vector, achieving error-free detection and a relatively high localization performance when the eavesdropper is in the vicinity of the legitimate transceiver pair. Inspired by data science, similar problems in other complicated channels can be solved as well provided that the training data is available and accurate [10].

Recently, the extension to the 3-D scenario is studied in [11], and the three-node MC network is considered as its 1-D and 2-D counterparts. Besides, the silent target (e.g., eavesdropper) remains an absorbing receiver, while the legitimate receiver is passive. The existence of the silent absorbing target affects the reception of the legitimate receiver, which can be reflected by the analytical channel impulse response (CIR). Based on the received signal vector, the transmitter-target and target-receiver distances can be obtained via the maximum likelihood estimation, realizing a relative localization of the silent target, whose performance can be further enhanced with extra receivers. Note that the distance between the legitimate transceiver pair is perfectly known in the schemes above, which can be achieved via the synchronization or channel estimation process. Despite being beneficial to the strategy of secure channel establishment, precise elimination of the eavesdropper can be achieved via the guard devices after the localization step.

Secret transmission strategy: Traditionally, encryption is deemed as one of the most secure methods paved for various communication systems. It relies on the secret keys governed by a reliable key management infrastructure and is typically applied in the upper-layer protocol. Thus, classical encryption may not be suitable for the MC network, where the research of the physical layer is still in progress, let alone the upper layers. Alternatively, variation of the physical channel enables the key-based encryption methods in the physical layer, which is detailed in the next section.

III. Safeguarding Molecular Communication Networks via PLS

PLS is an effective strategy for security enhancement that leverages the inherent features of the physical-layer communication channel from an information-theoretic perspective. It is not a competitor but acts as a complement to the conventional

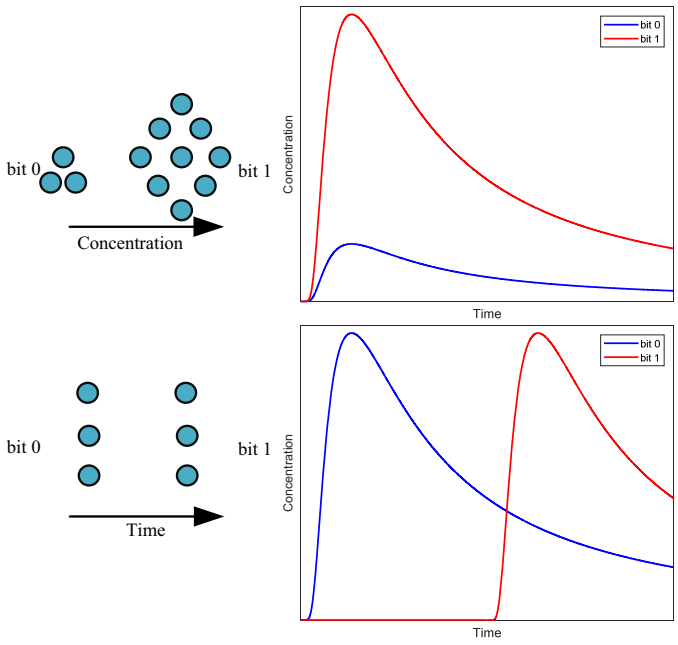

Fig. 3. CIRs with respect to different modulation schemes

encryption protocols in the upper layer. Current research on MC networks concentrates on the techniques in the physical layer rather than those in the upper layers. As a result, the classical encryption in conventional communication systems cannot be easily shifted to the MC system due to the lack of upper-layer protocols. The sufficiency of the physical layer research in MC, such as channel modeling, information theory, modulation, and signal processing, laid the foundation for PLS in MC networks, which is envisioned as a promising method for secrecy and privacy enhancement [2]. Moreover, the study of the physical-layer model facilitates the high-layer realization, such as the BioBlock, which is the blockchain mechanism for the secrecy improvement in IoBNT [12].

Despite having fruitful achievements in conventional communication systems, the PLS approaches in MC should comply with its system uniqueness. Compared with the computationally efficient devices in the conventional communication system, those in MC are usually energy-limited, especially for the micro-scale scenario. Additionally, biochemical property in MC leads to new challenges for secure signal processing techniques. Meanwhile, it brings opportunities as new features in the channel can be exploited for key generation. Two categories of PLS for MC, with or without key generation, are introduced as follows.

A. Keyless Security Strategy

Unlike the classical encryption schemes, keys are dispensable in certain PLS techniques, known as the keyless secure strategy. Sophisticated signal processing techniques, such as artificial noise, beamforming, and diversity, can be developed to ensure the secrecy of the MC networks. In the Alice-Bob-Eve model, Alice is the legitimate transmitter, whose intended

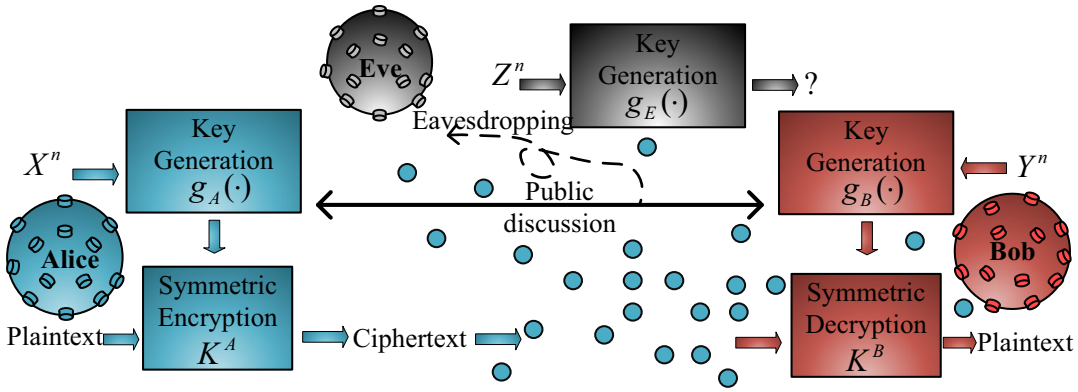

Fig. 4. Physical layer secret key generation in MC channel.

target is the legitimate receiver Bob, while Eve is the eavesdropper that intercepts the information from Alice to Bob. The secrecy performance is quantified via information leakage, i.e., the difference of the mutual information between the Alice-Bob and Alice-Eve links. The upper bound of the information leakage is called secrecy capacity realized by a specific distribution of the input symbols, namely, capacity-achieving distribution. The secrecy performance of the diffusion-based MC system with concentration shift keying (CSK) is analyzed from an information-theoretical point of view, providing two paramount secrecy metrics, i.e., secrecy capacity and secure distance [13]. However, only the estimation of lower bound secrecy capacity is derived as both links attain their channel capacity. The secrecy capacity highly depends on the system parameters such as the average signal energy, diffusion coefficient, and reception duration. Moreover, the distance between the transmitter and the eavesdropper is also an important aspect of secrecy performance. For both amplitude and energy detection schemes, secure distance is proposed as a secret metric, over which the eavesdropper is incapable of signal recovery.

Despite the case with CSK, the results of the secure metrics vary with the modulation type (e.g., pulse position, space, type) and reception mechanism (e.g., passive, partially absorbing, perfectly absorbing). For ease of understanding, Figure 3 depicts the modulation types and the corresponding CIRs with different reception mechanisms. Novel signal processing techniques and the biochemical channel properties can further assist the secrecy enhancement in the MC system. The molecular beamforming that avoids information disclosure can be realized via the flow generated in the channel. Besides, new dimensions of diversity, such as the aforementioned molecular diversity of ionic compounds, can be exploited. Note that the feasibility of these methods can be validated by the derived secrecy metrics.

B. Key-based Security Strategy

The rationale of key generation in the physical layer is kindled by the ideology of secret keys in the classical symmetric encryption method and the physical channel characteristics. The randomness in conventional wireless communication channels allows legitimate users to generate secret keys and exchange it without leaking to the eavesdropper. Thus, the key-based PLS only requires the channel characteristics of the legitimate link. It is a lightweight technique compared with its keyless counterparts, in which the channel state information of the eavesdropper is generally needed. Furthermore, MC is inherently abundant with randomness due to Brownian motion, time-varying biological environment, etc. As a result, the key-based PLS is more attractive for MC networks.

Tentative exploration of the molecular cipher key was first proposed in diffusion-based MC without resorting to the key management infrastructure [14]. Three fundamental properties, i.e., temporal variance, channel reciprocity, and spatial de-correlation are satisfied in this case. The mobility of the devices is one of the main factors that causes channel variation. In the macro-scale MC networks, the devices are mobile when attached to the external moving infrastructure. In the micro-scale MC networks, the motion of the nano-scale devices can be either random (e.g., Brownian motion) or actuated by motors [15]. As a result, the distance of the legitimate link is selected for key generation, whereas Alice and Bob mutually estimate the distance between them, while Eve cannot obtain the key based on its observations. Note that the fast time-varying channel mimics the one-time pad for secret keys, which is hard to be cracked by Eve. Besides, the diffusion-based MC system possesses channel reciprocity, and spatial de-correlation can be provided when Eve is incapable of following Bob. After randomness extraction, the quantization process maps analog measurements (e.g., distance) to binary bits based on the pre-defined thresholds and the quantization levels. The noisy observations in MC and the limitation of the nano-/micro-scale devices tend to secret key mismatch, degrading decryption performance in the legitimate link. To solve this problem, information reconciliation is the next stage that implements lightweight protocols or error-correcting codes for secret key correction, reducing the key disagreement rate, but some information may be leaked to Eve. By using the extractor or hashing functions, the privacy amplification stage allows Alice and Bob to distill the secret key, while Eve obtains a negligible amount of the information. As information reconciliation and privacy amplification appear together, a low-complexity joint design suitable for the MC system is necessary.

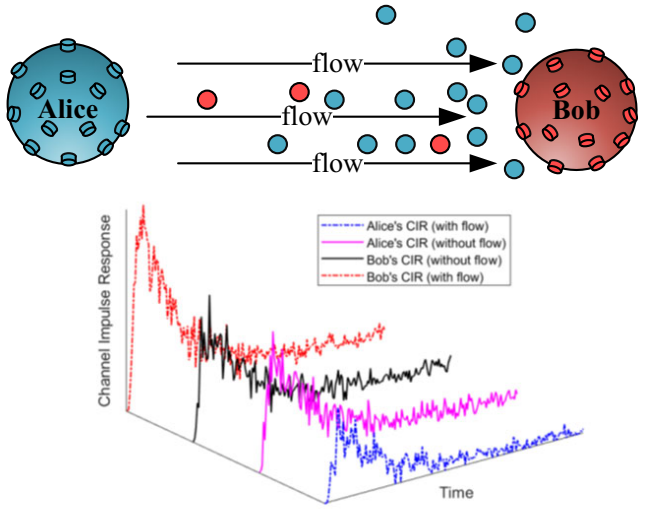

Fig. 5. Failure of channel reciprocity of advection-diffusion channel.

The feasibility of the key-based PLS for MC is reinforced by the observations from a macro-scale prototype, which can be scaled down to the micro-scale scenario [14]. Figure 4 illustrates the PLS with key generation for the MC network, where the blue circles are the information molecules over the MC wiretap channel.

IV. Open Challenges and Future Directions

There are still some open challenges for the security of the IoBNT with MC. Meanwhile, this section discusses some future research directions as well.

Complex channel characteristics: The IoBNT channel undergoes stochastic nature as a variety of mechanisms are involved, such as diffusion, background flow, and biochemical reaction. As a result, inter-symbol interference (ISI) and noise with signal-dependent variance are introduced to the IoBNT channel. The channel is highly complex whose model is hard to characterize and differs in both time and space dimensions. Against this background, it is hard to obtain the analytical solution of the secrecy capacity-achieving distribution that jointly considers both channel links. Motivated by the data-driven methods, machine learning techniques can be used to solve this problem provided with sufficient data [9]. Moreover, the channel reciprocity may not hold in some channels when the CIR or received signal strength is used as the random source for key generation. To be specific, as shown in Fig. 5, the noisy CIRs of the legitimate transceivers are approximately the same in the free diffusion channel (without flow), while they are asymmetric in the advection-diffusion channel due to the influence of flow. In this case, the channel parameters that are equivalent for both legitimate transmitter and receiver should be employed, e.g., distance.

Novel signal processing techniques: Unlike conventional communication systems, signals in MC have the constraint of being non-negative and real due to the discrete nature of the molecular particles. Besides, molecular signals are influenced by ISI and non-stationary noise. In this case, conventional secure techniques, including artificial noise generation, beamforming, etc., cannot be implemented for MC networks. The signal processing techniques in optical communication systems are mature due to their long history compared to those in MC, and they can be inspiring since both photonic and molecular signals share similar properties with respect to signal constraint and noise characteristics[10]. As MC bears the biochemical properties, the underlying cell signaling may provide novel signal processing methods against attacks and wiretapping, where interdisciplinary efforts are required to reach this goal.

V. Conclusions

Current research on MC networks mainly focused on signal transmission/reception in the physical layer. However, security issues are also of great importance in the MC networks (e.g., IoBNT), while its study is neglected in the literature. In light of this, this article presented the looming threats underlying the MC networks. Then, the biochemical counterattack strategies inspired by nature in multi-scale scenarios are exemplified. The security approaches can be easily achieved via the PLS manner without the involvement of high-layer encryption, which is reasonable for MC networks due to the lightweight implementations. Then, both the keyless and key-based PLS schemes for MC networks were discussed from the perspective of data science and conventional model-based techniques. Finally, some open problems and future directions for secrecy enhancement in MC networks are envisaged, which suggests that interdisciplinary efforts are required to reach this goal.

References

[1] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The Internet of Bio-Nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015.
[2] L. Mucchi *et al.*, "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.
[3] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Commun. Netw.*, vol. 3, no. 3, pp. 151–160, Sept. 2012.
[4] V. Loscrí *et al.*, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 198–207, Sept. 2014.
[5] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in bio-NanoThings communication networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 665–676, Apr. 2016.
[6] T. Kawakami and K. Kasakura, "Mast cell eavesdropping on bacterial communications," *Cell Host & Microbe*, vol. 26, no. 1, pp. 3–5, July 2019.
[7] H. B. Yilmaz, G.-Y. Suk, and C.-B. Chae, "Chemical propagation pattern for molecular communications," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 226–229, Apr. 2017.
[8] W. Guo *et al.*, "Eavesdropper localization in random walk channels," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1776–1779, Sept. 2016.
[9] O. D. Kose *et al.*, "Machine learning-based silent entity localization using molecular diffusion," *IEEE Commun. Lett.*, vol. 24, no. 4, pp. 807–810, Apr. 2020.
[10] Y. Huang *et al.*, "Signal detection for molecular communication: Model-based vs. data-driven methods," *IEEE Commun. Mag.*, vol. 59, no. 5, pp. 47–53, May 2021.
[11] X. Bao *et al.*, "Relative localization for silent absorbing target in diffusive molecular communication system," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5009–5018, Apr. 2022.
[12] S. Misra, S. Pal, and A. Mukherjee, "Bioblock: A blockchain analogous mechanism for integrity in IoBNT-based drug delivery systems," *IEEE Syst. J.*, pp. 1–8, 2022.

[13] L. Mucchi *et al.*, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, pp. 110 687–110 697, 2019.
[14] W. Guo *et al.*, "Secure Internet-of-Nano things for targeted drug delivery: Distance-based molecular cipher keys," in *Proc. IEEE Middle East and Africa Conf. on Biomed. Eng.*, Amman, Jordan, Oct. 2020, pp. 1–6.
[15] J. T. Foy *et al.*, "Dual-light control of nanomachines that integrate motor and modulator subunits," *Nature Nanotechnol.*, vol. 12, p. 540–545, June 2017.

Yu Huang received the Ph.D. degree from South China University of Technology, China, in 2021. He is currently an Associate Professor with Guangzhou University. His main research interests include molecular communications, physical layer security, and emerging communication techniques.

Miaowen Wen received the Ph.D. degree from Peking University, China, in 2014. He is currently a Professor with South China University of Technology, China. He has published 2 books and more than 180 IEEE journal articles. His research interests include a variety of topics in the areas of wireless and molecular communications.

Lin Lin received his B.Eng., and M.Eng. degrees from Tianjin University and Ph.D. from Nanyang Technology University, Singapore. He is an associate professor at Tongji University, China, and was a Marie-Curie Fellow at the University of Warwick on the Internet of Molecular Nano-Things. His fellowship focuses on integrating fluid dynamics with information theory, through developing synchronization and modulation schemes that exploit fluid dynamic knowledge.

Bin Li received the Ph.D. degree in communication and information engineering from the Beijing University of Posts and Telecommunications (BUPT) in 2013. He is currently an Associate Professor with the School of Information and Communication Engineering of BUPT. His current research interests include statistical signal processing for communications, such as molecular communications, millimeter-wave communications, UAV communications, MIMO communication/radar systems.

Zhuangkun Wei received the Ph.D. degree in engineering from the University of Warwick, U.K., in 2021. His research interests cover physical layer security, graph signal processing, molecular communications, and Explainable Artificial Intelligence (XAI). He is currently a research fellow in the School of Aerospace, Transport and Manufacturing, Cranfield University.

Dong Tang received the Ph.D. degree from Sun Yat-sen University, Guangzhou, China, in 2007. He is currently a Professor with Guangzhou University, Guangzhou. His interests are in the areas of energy harvesting in wireless communication networks and wireless MIMO and OFDM communication networks.

Jun Li received the Ph.D. degree from Chonbuk National University, Jeonju, South Korea, in 2016. He is currently an Associate Professor with Guangzhou University, Guangzhou, China. He has published more than 50 papers in refereed journals and conference proceedings. His research interests include spatial modulation and OFDM with index modulation.

Wei Duan Wei Duan received the Ph.D. degree from Chonbuk National University, Jeonju, South Korea, in 2017. He is currently a full Professor with Nantong University, Nantong, China. His research interests include a variety of topics in the areas of wireless communications.

Weisi Guo received his M.Eng., M.A., and Ph.D. degrees from the University of Cambridge. He is Chair Professor of Human Machine Intelligence at Cranfield University. He has published over 150 papers and is PI on over 12 research projects from EPSRC, Royal Society, EC H2020, and InnovateUK. His research has won him several international awards (IET Innovation 15, Bell Labs Prize Finalist 14 and Semi-Finalist 16 and 19). He is a Turing Fellow at the Alan Turing Institute and a Fellow of the Royal Statistical Society.

Physical-layer counterattack strategies for the internet of bio-nano things with molecular communication

Huang, Yu

2023-06-06

Huang Y, Wen M, Lin L, et al., (2023) Physical-layer counterattack strategies for the internet of bio-nano things with molecular communication, IEEE Internet of Things Magazine, Volume 6, Issue 2, June 2023, pp. 82-87

https://doi.org/10.1109/IOTM.001.2300029