Review of Physical Layer Security in Molecular Internet of Nano-Things

Song Qiu, Zhuangkun Wei, Yu Huang, Mahmoud Abbaszadeh, Jerome Charmet, Bin Li, Weisi Guo

***Abstract*—Molecular networking has been identified as a key enabling technology for Internet-of-Nano-Things (IoNT): microscopic devices that can monitor, process information, and take action in a wide range of medical applications. As the research matures into prototypes, the cybersecurity challenges of molecular networking are now being researched on at both the cryptographic and physical layer level. Due to the limited computation capabilities of IoNT devices, physical layer security (PLS) is of particular interest. As PLS leverages on channel physics and physical signal attributes, the fact that molecular signals differ significantly from radio frequency signals and propagation means new signal processing methods and hardware is needed.**

Here, we review new vectors of attack and new methods of PLS, focusing on 3 areas: (1) information theoretical secrecy bounds for molecular communications, (2) key-less steering and decentralized key-based PLS methods, and (3) new methods of achieving encoding and encryption through bio-molecular compounds. The review will also include prototype demonstrations from our own lab that will inform future research and related standardization efforts.

***Index Terms*—Molecular Communications; Physical Layer Security; Secret Key Generation; Internet of Nano-Things**

I. Introduction

Over the past few decades, the sizes of electronic devices have shrunk by several orders of magnitude. One consequence of increasing miniaturization is that we can now carry, wear, and embed advanced machinery on or inside ourselves. The World Economic Forum identified nano-scale Internet-of-Things (IoT) as a top 10 emerging technology and efforts to standardize the communication network technology have been underway since 2015 under IEEE P1906.1 [1].

This work is supported by the EPSRC TAS-Security node (EP/V026763/1, 2020-24), USAFOFSR MolSig (FA9550-17-1-0056, 2017-21), the Royal Society Small-Talk (IE150708, 2015-17). the National Natural Science Foundation of China under Grant 62201161, the Tertiary Education Scientific research project of Guangzhou Municipal Education Bureau under Grant 202235019. No new data were created or analysed in this study. Data sharing is not applicable to this article. (Corresponding author: Weisi Guo, weisi.guo@cranfield.ac.uk)

Song Qiu is with the School of Physical Science and Technology, Southwest Jiaotong University, Chengdu, 610031, China.

Zhuangkun Wei is with the School of Aerospace, Transport, and Manufacturing, Cranfield University, MK43 0AL, UK.

Yu Huang is with the Research Center of Intelligent Communication Engineering, School of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China

Mahmoud Abbaszadeh is with Imperial College, London, SW7 2AZ, UK.

Jerome Charmet is with Warwick Medical School, University of Warwick, Coventry, CV4 7AL, UK; and Haute Ecole Arc, Switzerland.

Bin Li is with the Department of Information Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

Weisi Guo is with the School of Aerospace, Transport, and Manufacturing, Cranfield University, MK43 0AL, UK, and also with the Alan Turing Institute, London, NW1 2DB, UK.

Current IoT systems are silicon-based hardware that process mainly electrical and electromagnetic signals - the basis for storage, communication, and computing. The scalability (cost, energy, size) of current silicon-based IoT devices does not meet all of our emerging and future demand. For example, embedded in-vivo IoT systems for healthcare often need to be bio-compatible and transmit signals in compact cellular environments. These so-called Internet of Nano-Things [2] have particularly unique signal processing and communication security challenges which we will explain later. At the basic level, the complex biological environment often weakens electromagnetic signals and puts strict restrictions on radiation. Furthermore, nanotechnology device dimensions shorten the wavelength to the THz regime and this puts further constraints on transmission range and efficient signal processing.

Hence, research has been motivated by molecular-based communications, which is prevalent in nature across multiple scales (e.g., from intra-cellular to inter-species level). For example, we already know that artificial DNA data systems promise to reduce encoding and storage costs by 100x for the same capacity and endurance performance [3]. They also offer new secrecy, bio-compatibility, and resilient networking paradigms - as we will see throughout the rest of the review paper. Therefore, there is tremendous excitement to understand the signal processing of Internet-of-Nano-Things (IoNT) networking [2], [4], [5].

As previously mentioned, the application of IoNT in healthcare especially is far-reaching: the ability to monitor a variety of physical and biochemical states (i.e., wound recovery [6], chrono drug delivery [7], localization [8], and coordinated micro-surgery. There are a few competing technologies for nano-communication for IoNTs (e.g., THz, magnetic induction), but our primary focus in this review is molecular communications. Beyond healthcare, there are a variety of heavy industry and defence & security use cases [9] and molecular networking could be a new air interface for 6G Beyond [10]. In recent years, up-scaled experimentation has provided some of the foundations for bridging theory and practice in molecular communications for IoNT (see review in [9]).

A. Existing Cybersecurity Reviews

This review paper is focused on the unique signal processing techniques needed to ensure there are secure molecular communications (MC). It is envisaged that IoNT devices have low computation and energy, therefore they need to have a flat computing architecture and simple security architectures,

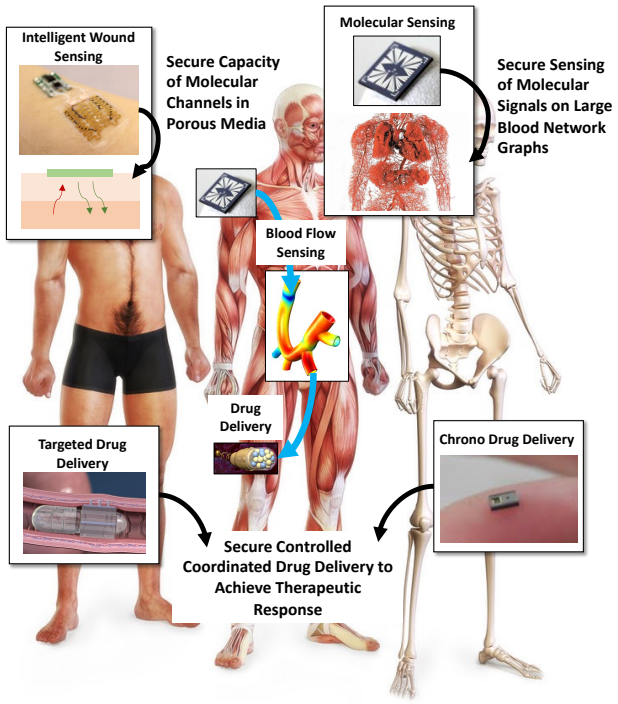

Fig. 1. Molecular communications can connect different Internet-of-Nano-Things (IoNT) to create a chrono-synchronized health monitoring and drug delivery ecosystem. Security risks presented by new molecular information physical channel is a new research frontier.

which differentiates themselves from traditional electronic cybersecurity which is a multi-layered approach (e.g., separate modules and layers against spoofing, authentication, communication errors, and eavesdropping). As such, physical layer security (PLS) presents an ideal framework to leverage on the physical signal vectors to improve security. Our review primarily focuses on the PLS aspects of MC [11]. We will see throughout the paper how different propagation physics (e.g., molecular diffusion-advection vs electromagnetic radiation) affect signal processing, cybersecurity risk profile, and mitigation design.

Existing reviews in MC generally do well in identifying the proprietary challenges faced by nano-machines in a contained biological environment. In one of the first MC cybersecurity reviews in 2012 [12], it was reviewed that disrupting the molecular propagation pathways is likely to be the most effective form of attack (e.g., saturating the chemical signaling channels with a biochemical agent or interfering with the biophysical propagation mechanisms such as blocking bio-membranes). Therefore for the attacker, without access to the bio-environment and its own set of capable nano-machines, the disclosure, deception, and usurpation risks are relatively small, whereas the disruption risks are relatively much larger.

Penetration attacks with the insertion of equivalent or superior IoNT devices create new attack vectors and relevant research. For example, one would be interested in the achievable information theoretic secrecy rate for a given distribution of unknown eavesdroppers [13], [14], how to detect information leakage and infer the location of eavesdroppers [15], and the potential for innovative biochemical cipher keys. These topics will be the focus of the review in this paper. On the one hand, we can borrow a great deal of knowledge from the decades in wireless security to provide a physical layer security (PLS) framework, which was discussed in the first review in this area [16], but we must also develop new techniques to encrypt molecular messages, which has not been researched sufficiently.

The aforementioned 2 attack areas of disruption and secrecy rate leakage raise new communication theory and signal processing research:

- **robust and efficient channel estimation signal processing** to counter unexpected changes in channel physics. Local biochemical and biophysical changes can lead to incorrect channel state information (CSI) estimation which can cause a wide range of issues from decoding errors to inconsolable PLS key generation.
- **reduce information leakage rate** to counter hidden eavesdroppers and improve the secure information capacity of the channel. Here, the completely different propagation physics of MC lends to new analysis and signal processing requirements compared to radio communications.

B. Gaps in Review Knowledge & Contributions

Current cybersecurity reviews in molecular communications are very few. We found only 2 dedicated reviews more than 8 years old [12], [16], and a recent general review on MC that touched on cybersecurity [17]. New cybersecurity research is rapidly emerging, and a review of their progress and future research areas is needed.

Here, we take a information theory and communication signal processing led review of the cybersecurity research opportunities in molecular communications, primarily at the physical layer level. Our review is organised as follows (see Fig.2), spanning different technology complexity and security capabilities:

- Overview of threat regions and consequences for IoNT molecular communications (Section II)
- Quantitative review and analysis of the information-theoretic molecular secrecy and leakage rate, as well as mitigation strategies (Section III)
- Review of molecular physical layer security techniques that exploit diffusion-advection propagation physics (Section IV)
- Discuss and review future research in this area, such as DNA-based molecular encryption techniques (Section IV)

To highlight the novel differences between PLS in molecular communications compared to radio frequency (RF), we explain in Section II that the biophysics propagation is different and the signal feature space is also different. In RF, we leverage on the IQ diagram (e.g., phase, magnitude). Recent research in RF focus on developing transforms and neural networks that can cancel out channel variations to uniquely create robust authentication fingerprints or cipher keys. In molecular communications, we must identify new features and signal processing transforms that are robust to new channel variations

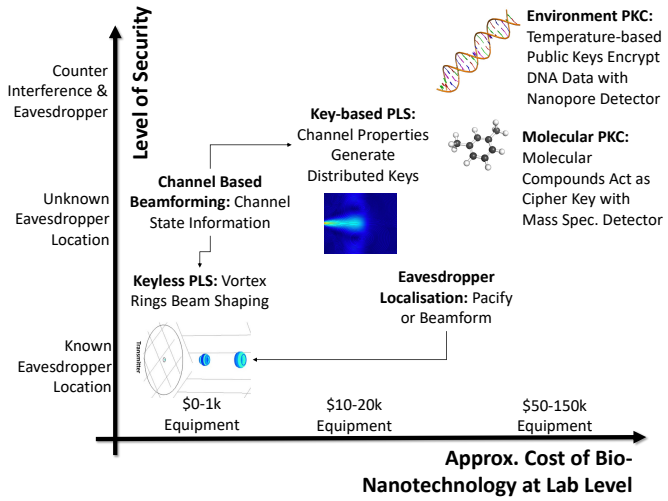

Fig. 2. Review paper focuses on molecular communication security, ranging from keyless and key-based physical layer security (PLS) to Public Key Cryptography (PKC) using Molecular Compounds. These Incur Different Laboratory Costs in Equipment and Security Capabilities.

(e.g., diffusion-advection currents). This requires both new signal processing and communication theory frameworks and hardware for achieving it. As a result, the achievable bounds in secrecy and key rate are different (see Section III-IV). In Section V, we further exploit biochemical aspects of molecular communications for security by examining features of protein or DNA molecules, and how a shared environmental condition between transmitter and receiver can act as a non-digital cipher key to encrypt data. A small lab demonstration is shown, which we believe is reasonably novel and we hope the editor and reviewers find this interesting as a motivation for further research.

II. Cybersecurity Overview for Molecular IoNTs

A. Bio-informatic Channels Transform Security Challenges

PLS (in both radio-based and molecular-based communications) requires the derivation of security properties from the physical signal and channel. We review here the key differences between classical RF wireless channels and molecular signal channels, which are [26], [27]:

1) Externally Controlled Propagation: radio signal directionality in radio frequency is controlled by the transmitter (e.g., beam-steering, beam-forming), whereas molecular signal directionality is largely controlled by the channel dynamics (e.g., co-flow, vortices) because high frequency features that gives rise to molecular signal directionality rapidly lose momentum after emission via the diffusion and mixing process. As such, RF signal loses power according to distance $\propto d^{-\alpha}, \alpha = 2-4$, whereas molecular signal loses power according to $\propto \exp(-d^2)/d^{\beta}, \beta = 0.5{-}1.5$ [28]. This means that whilst RF signal processing can rely on high frequency signal features, molecular signal processing cannot, and must rely on alternative features such as vorticity (see Section IV).
2) Reactive Interference: radio signal interference is determined by the co-frequency of the carrier band, whereas molecular signals are determined by the chemical compound and how it reacts with other compounds. Therefore, the surrounding environment in RF simply acts as passive reflection or absorbing surfaces - contributing to a multi-path and attenuation effect. On the other hand, a biological environment in molecular communications can entrap, delay, or even alter the signal through reactions and complex interactions.

As such, whilst some of the basic threat vector notions of eavesdropping, spoofing, and jamming apply to molecular communications, these notions require careful thought and rework in the context of new channel models and signal modulation constellations. For example, diffusion-advection propagation means eavesdropping in the distance is far less likely, but interference from a wide range of reactive chemicals [29] and biological predation (e.g., bacteria eating RNA signals) means a transport host is often needed [30]. It is in this light that we qualitatively review the current cybersecurity papers in the literature below, as well as identify new threat vectors and opportunities for wireless research.

B. Review of Threat Vectors and PLS

In current autonomous systems and IoT systems, jamming and spoofing account for over 75% of attack vectors and this is largely conducted on the wireless and guidance systems [31]. However, the landscape for how attackers will disrupt nano-scale molecular IoNT remains unknown. We broadly review molecular IoNT security within the STRIDE landscape first to get a broad understanding, before focusing on why PLS is important:

1) **Information Disclosure:** molecular propagation inside a body makes disclosure and leakage possible, but the survival of meaningful and complete molecular signals in the wild is challenging. Research in this space (Reviewed in Section III) focuses on quantifying the secrecy rate and leakage rate for a wide range of propagation channels and noise distributions, developing new molecular communication measures for secrecy rate loss, as well as developing signal processing mechanisms to mitigate information leakage.
2) **Spoofing or Repudiation:** IoT devices are unlikely to carry sophisticated authentication and destination tags and will therefore be vulnerable to spoofing attacks that inject artificial signals to falsify information. Therefore, low-cost PLS that secures messages is critical. Research in this space (Reviewed in Section IV) focuses on developing robust signal feature extraction for low-complexity devices to aid robust channel estimation and cipher key generation. Emerging research (reviewed as future work in Section V) also focuses on molecular-level encoding to reduce the risk of spoofing.
3) **Jamming:** jamming or interference of molecular signals with similar or reacting agents remains a highly likely form of attack through both the diet and the environment interaction with bodies [20]. However, it is also a very

TABLE I
MOLECULAR IONT THREAT VECTORS AND REFERENCES: INTERNAL/EXTERNAL ATTACKERS AND USING/TARGETING IONT NODES. A × SIGN INDICATES THERE IS NO SUITABLE SIGNAL PROCESSING RESEARCH IN THIS AREA, AND A ✓ SIGN INDICATES ACTIVE RESEARCH WITH A BRIEF DESCRIPTION AND CITATION - WHICH IS EXPLAINED IN MORE DETAIL IN SECTION II.

Research Area / Attack Vectors	Secure Capacity [18] (Section III)	Physical Asset Security (Section IV & V)	Key-based Physical Layer Security (Section IV)	Cryptography Security [19]
External Interference Attack [20]	✓Achievable Legitimate Rate [18], [21], [22]	✓Novel Molecular Modulation [3]	× Vulnerable to Low SNR and Eve Location [23]	✓
Injection of IoNT Bots for Elevated Privilege	×	✓Difficult to Copy Mass Spec Signature [24]	× Transmitter Signature Will Erode	× Vulnerable to Stronger Attacker
Eavesdrop [23] of Device / Channel Info	✓Achievable Secure Rate	×	✓Unique secret key generation [25]	× Vulnerable to Stronger Attacker

invasive and potentially harmful attack method which we do not review in this paper.

4) **Tampering or Elevation of Privilege:** is not likely given the embedded nature of IoNT devices and the relatively high technological requirement for their reconfiguration or tampering or elevation of privilege to control communications. This requires insertion, localization [32], evading anomaly detection [33], and tampering to be jointly successful.

There are a myriad of detailed scenarios on how molecular-based IoNT systems can be attacked and we detail their corresponding recent research in Table I. We can see that when we divide them into whether they rely on internal IoNT help or not, and whether the IoNT is part of the adversarial threat or merely a target: we can see that most of the threat either involves internal IoNT friendly actors or large-scale external attacks. As such, our review targets the following novel research areas: (1) maximizing molecular secrecy rate between internal IoNT devices (Section III), (2) generating cipher keys through low-cost common channel features (Section IV), and (3) emerging future research in molecular level encoding (Section V).

III. KEY-LESS SECURITY

Key-less PLS exploits spatial-temporal knowledge of either the legitimate receiver and/or the eavesdroppers to prevent a number of attacks. In radio-based communication, knowing the eavesdropper(s)' locations (distributions) traditionally allows multi-antenna systems to perform beam-steering to reduce information leakage to Eve or angular momentum modulation to distort side-beam data leakage to Eve. However, in molecular communications, this can only be done when there is assistance from channel flow or at very close distances [34], or with specially generated vortex rings, which is uniquely propagates molecular signals over long distances and can be guided by infra-red beams [35].

A. Secrecy Rate Bounds

Unlike RF communications, molecular eavesdropper localization is uniquely possible in molecular communications because the number of molecules a receiver has to absorb usually [15], [23] (e.g., even passive optical receivers can still trap molecules). Furthermore, if the channel state information (CSI) is known (e.g., molecular channel co-flow properties), one can maximize the secrecy rate via the following secrecy capacity analysis, which we review below.

Secrecy rate analysis is particularly relevant when a malicious insider IoNT is used to eavesdrop on other legitimate IoNT data (see Table I) [36], collect channel state information (CSI) [37], as well as hardware information (e.g., fingerprint device transmitter characteristics [38]). The achievable secrecy rate (secrecy capacity or secrecy loss [22]) of molecular IoNT devices depends highly on the transmitted molecular signal volume, the location (or location distribution) of the eavesdroppers, and how absorbing its receiver is relative to those of Alice and Bob. This analysis has been recently performed for a variety of secrecy loss metrics [22] and for different bio-inspired channel geometries [18].

Combining the information-theoretic security with the specific molecular channel models, the secrecy capacity predominately scales as follows [13], [14]:

$$C_S \propto \begin{cases} -\log_2\left[\frac{d_e}{d_l}\right]^2 + (d_e - d_l) & \text{Concentration channel} \\ \log_2 \frac{d_l}{d_e} & \text{Timing channel} \end{cases} \tag{1}$$

where d_l and d_e are the communication distance between the legitimate receiver and Eve receiver. In Eq. (1), the expression of the secrecy capacity C_S is different in concentration and timing MC channels, whereby the former uses the number of molecules to convey information bits, whereas the latter modulates the information bits via the release time of the molecule.

The work is recently extended to general Gaussian distribution of eavesdropper locations (e.g., unknown but large no. of IoNT devices follow some distribution) [21] and also a prediction algorithm for the hidden location of Eve given it is absorbing [15]. This enables the potential of then localizing the eavesdropper(s) and either pacifying it or allowing beamforming to reduce information leakage.

As a proof-of-concept simulated demo, we designed a mobile IoNT scenario where Bob and Eve continuously move (Bob randomly in a Gaussian-distributed fashion, and Eve rotates around Bob). In Fig. 3 we show the molecular IoNT secrecy capacity [14] variation with total channel capacity and

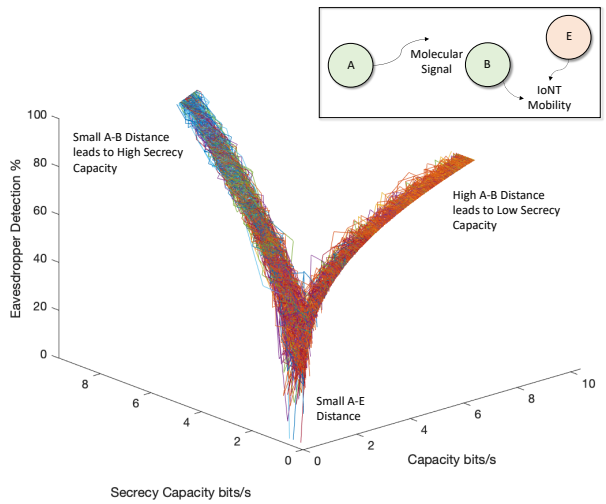

Fig. 3. Molecular IoNT secrecy capacity variation with channel capacity and eavesdropper detection chance. Randomness is generated via the mobility of nodes and diffusion-advection channels.

eavesdropper detection chance [15], [39]. This is different from radio communications because passive Eve detection is possible due to the absorbing (chemical reaction) nature of molecular communications. We used the results in [14] to demonstrate a bifurcation in the secrecy capacity and eavesdropper performance with 3 zones of interest: (1) when Eve is very close to Alice and the A-B secrecy capacity and capacity are both close to 0, e.g., then the ability for Bob to detect Eve is minimal due to high noise to signal ratio estimation issues, (2) when Alice is close to Bob and we can achieve both high secrecy capacity and total capacity, and (3) when Alice to Bob distance is high and whilst some reasonable total capacity can be achieved, it is sensitive to Eve and the secrecy capacity is low. What remains to be done is a more representative analysis of the secure information capacity of complex fluid dynamic channels representative of obstacle-rich in-vivo environments (e.g., the conditional mutual information of Reynolds Averaged Navier-Stokes dynamics).

B. Maximizing the Secrecy Rate

To maximize the secrecy rate in MCs, current researches depend on whether the instantaneous CSIs of legitimate and malicious users are known.

1) Known Molecular CSI: When such CSIs are known, [14] provides a secure distance d_E, by identifying the number of transmitted particles, Q, so that any Eve that is d_E far from legitimate Tx cannot measure the number of particles that is more than the detection threshold γ, i.e.,

$$\frac{Q}{4\pi D d} \leq \gamma, \ \forall d > d_E. \tag{2}$$

2) Unknown Molecular CSI: In the absence of the instantaneous CSIs of legitimate and malicious receivers, directly maximizing the secret rate is of great difficulty. Instead, sub-optimal metrics are designed by [13], [40], which are reviewed in the following.

(i) **Maximum achievable fractional equivocation** (MAFE) is generally used to characterize the decoding error probability of Eve, and is defined as:

$$\Delta = \begin{cases} 1 & R_S \leq C_S \\ \frac{C_S}{R_S} & 0 < C_S < R_S \\ 0 & C_S \leq 0 \end{cases} \tag{3}$$

where R_S is the actual secrecy rate. By taking Eq. (1) into Eq. (3), MAFE for MCs is obtained, which links Eve's error with parameters like R_S, d_l, and R_B (the transmitting rate).

(ii) **Generalized Secrecy Outage Probability** (GSOP) is defined as the probability that the MAFE is less than a small threshold, i.e., $\mathbb{P}(\Delta < \bar{\Delta})$. This indicates the probability of Eve's small decoding errors is limited by $\bar{\Delta}$. Then, optimal parameters of legitimate nodes can be derived by:

$$\begin{aligned} &\min_{R_S, R_B, d_l} \mathbb{P}(\Delta < \bar{\Delta}) \\ &\text{s.t. } R_S \cdot \mathbb{P}(R_B \leq C_B) > \Gamma, \ R_S, R_B, d_l > 0. \end{aligned} \tag{4}$$

Here, C_B is the channel capacity of the legitimate channel, and $R_S \cdot \mathbb{P}(R_B \leq C_B)$ represents the throughput that has to be greater than a required threshold Γ.

(iii) **Average Fractional Equivocation** (AFE) represents Eve's overall decoding error probability, which is expressed as $\mathbb{E}(\Delta)$. AFE provides another security metric, which gives legitimate parameters by maximizing its value but with required legitimate throughput, i.e.,

$$\begin{aligned} &\max_{R_S, R_B, d_l} \mathbb{E}(\Delta) \\ &\text{s.t. } R_S \cdot \mathbb{P}(R_B \leq C_B) > \Gamma, \ R_S, R_B, d_l > 0. \end{aligned} \tag{5}$$

(iv) **Average Information Leakage Rate** (AILR) gives an expression of $I(X;Z)$ via the definition of MAFE, i.e., $I(X;Z) = \mathbb{E}((1-\Delta) \cdot R_S)$, which represents the amount of information that is leaked to Eve at rate R_S. Leveraging AILR, the optimal configuration of legitimate parameters should minimize the information leakage but hold the required legitimate throughput, i.e.,

$$\begin{aligned} &\min_{R_S, R_B, d_l} \mathbb{E}((1-\Delta) R_S) \\ &\text{s.t. } R_S \cdot \mathbb{P}(R_B \leq C_B) > \Gamma, \ R_S, R_B, d_l > 0. \end{aligned} \tag{6}$$

IV. Key-based Security: Exploiting Common Physics

Developing physical layer wireless key-based security is particularly relevant when there are external channel attacks or eavesdroppers (Table I), and more bio-inspired robust methods to secure the molecular messages at the channel level are required (see Section IV).

Key-based security uses mutual channel properties between IoNT nodes to create distributed cipher keys without public key cryptography requirements [19]. At an authentication level, unique channels can be used to accept or reject IoNT devices as a way to fingerprint their location dependent channel [45], however this can prove unreliable in real dynamic channel environments where the channel changes or the location varies. For key-based PLS in traditional wireless systems, we

TABLE II
PHYSICAL LAYER SECURITY DIFFERENCES BETWEEN MOLECULAR AND RADIO IOT DEVICES

	Propagation Physics	Common Signal Features	Key Generation & Reconciliation	Receiver Hardware	Observation Hardware
Radio Communications	Maxwell wave propagation, ray tracing	IQ Map, Differential Constellation Trace Figure (DCTF) [41]	Slepian-Wolf & Secure Sketch [42], AES	Software Defined Radio	Oscilloscope
Molecular Communications	Fick's diffusion-advection [43], Navier-Stokes	Curl of Co-Flow Vorticity, Distance Estimation [25]	Reconciliation [25]	Nanopore, Optical Sensor	Particle Image Velocimetry [44]

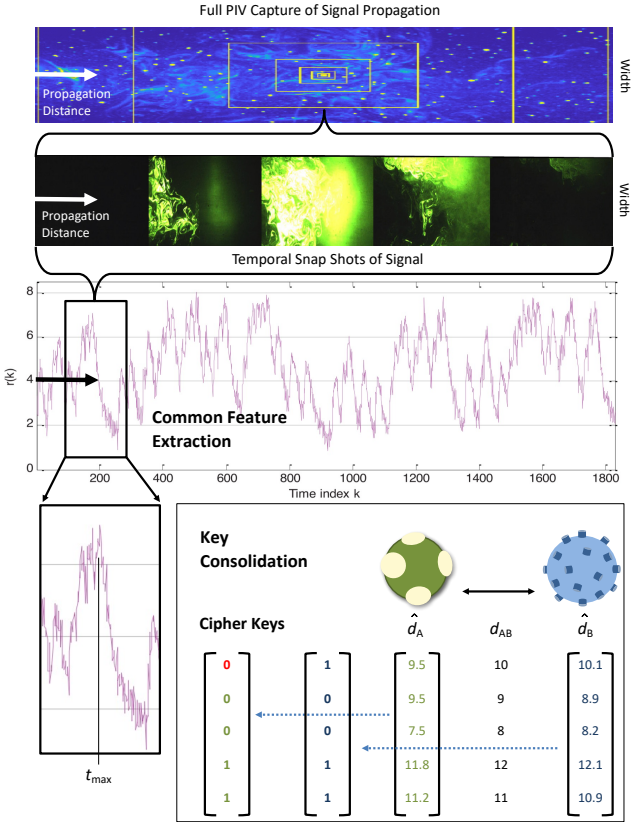

Fig. 4. Our Proof-of-Concept: (top) PIV captures the molecular signatures (middle) feature extraction using high-dimensional embedding to create rich signatures, and (bottom) key consolidation between legitimate users Alice and Bob [25].

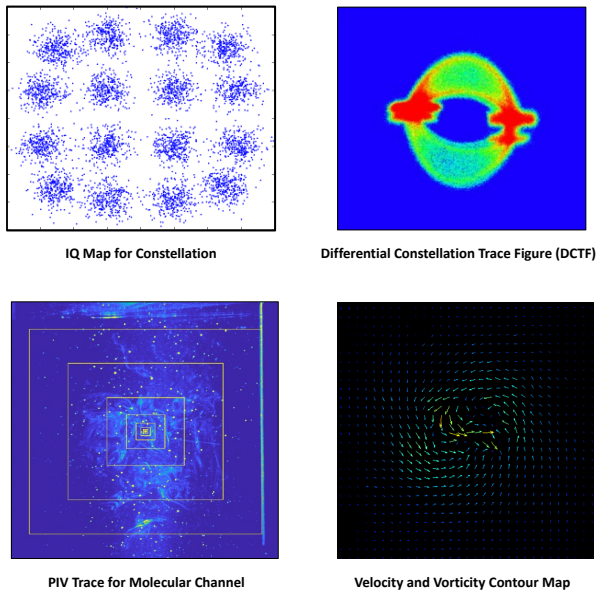

Fig. 5. Example of feature maps that are used in PLS. (top) radio PLS uses features extracted from IQ constellation map or the DCTF [41] to produce a feature set. (bottom) molecular PLS uses features extracted from PIV traces and velocity/vorticity contours [44].

have reciprocal channels and use features such as modulation patterns [46].

In molecular IoNTs, we are expected to use molecular signals in realistic non-isotropic fluid dynamic channels, which are non-reciprocal and can be subjected to dynamic advection forces that reduce the communication coherence time. This on the surface rules out physical layer secret key generation which typically relies on reciprocal channels. However, the non-reciprocal channel between Alice and Bob still shares properties that are dynamic, common, and unique, which can be teased out.

We give a comparison of radio and molecular PLS key differences in Table II and showcase some example feature maps used in radio communications and molecular communications in Fig. 5. RF-based PLS uses features extracted from IQ constellation map or the Differential Constellation Trace Figure (DCTF) [41] to produce a feature set. (bottom) molecular PLS uses features extracted from PIV traces and velocity/vorticity contours [44]. In molecular communications, the common features can be the ambient co-flow velocity and vorticity field, unique to each spatial channel. That is to say, X-to-Eve would yield different co-flow fields to Alice-to-Bob. Exploiting this, one can design the PLS cipher key generation process in 3 stages (see Fig. 4 for real laboratory demonstration of molecular PLS):

1) Alice and Bob try to converge on a common estimation of the ambient co-flow velocity and vorticity field between them. High-dimensional metric combining techniques can be used to enrich the features [47]
2) Remove estimation noise and create feature embeddings to generate a key.
3) Generate on a common cipher key based on their correlated but imperfect channel estimates by employing Slepian-Wolf source coding for example. Then add an information reconciliation stage to reach an agreement (e.g. secure sketch technique) and privacy amplification

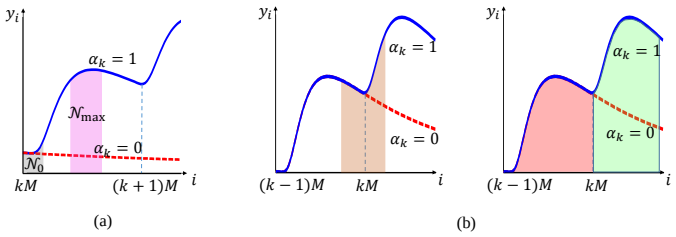

Fig. 6. Illustration of sub-metrics that contribute to a high-dimensional feature. (a) gives the local rising edge metric, whilst (b) shows the successive properties that contain the inflexion metric and the energy difference.

with AES implementation [25].

A. Low-Complexity High-Dimensional Molecular Signal Feature Extraction

As the realistic molecular communication channel is often unknown, existing coherent schemes (e.g., the state-of-the-art maximum a posteriori, MAP) have to pursue complex channel estimation and ISI mitigation techniques, which will result in either high computational complexity, or poor estimation accuracy that will hinder the detection performance. For the secret key generation in the physical layer, existing common feature extraction can be categorized into two families.

1) Data Driven CSI Estimation: The first family relies purely on the legitimate CSI or channel-related parameters measured by two legitimate nodes. This includes the feature constructed directly by estimated CSI [48], [49], or the mathematical combinations of the received signals to further depress the noise or inter-symbol interference (ISI) effects [47], [50]. Specially, the work in high-dimensional feature extraction designs in [47] provides a high-dimensional feature extraction, which is able to resist noise and ISI, and further contains most of the channel randomness by its high-dimensional structure. Many unique features of the transient effects of molecular signal propagation are different from radio signals, such as (see Figure6) [47]: (1) the local rising edge metric when a molecular pulse first arrives at the receiver, and (b) the successive properties that contain the inflexion metric and the energy-difference. The realization of this high-dimensional non-coherent scheme is to use a Parzen window technique-based probabilistic neural network (Parzen-PNN). Parzen-PNN has the ability to approximate the multivariate posterior densities by taking the previous detection results into a channel-independent Gaussian Parzen window, thereby avoiding the complex channel estimations. The complexity of the posterior computation is shared by the parallel implementation of the Parzen-PNN. By deducing the theoretical bit error rate (BER) for any constructed high-dimensional non-coherent metric, the authors in [47] proved that higher dimensionality always achieves a lower BER in the same sample space, at the expense of higher complexity on computing the multivariate posterior densities. Leveraging these methods, common features of two legitimate nodes can be obtained for physical layer secret key generation.

2) Randomness Injection Methods: The second family exploits not only the channel randomness but also induces extra entropy from the signal space. From the theoretical point of view, this includes one-way and two-way randomness injections. The one-way randomness injection refers to one legitimate node (Alice) transmitting a random signal and the other one (Bob) transmitting a public pilot sequence. Then, the common feature is Bob's received signals, which can also be constructed by Alice via the combination of the transmitted random signal and the estimated legitimate CSI. In comparison with the pure CSI-based feature, such a one-way randomness feature contains more entropy from not only the channel randomness but the random signal space induced from one legitimate node, therefore capable of providing a higher secret key rate (SKR) to secure the communication channel.

Then, to further speed up the SKR, two-way randomness injection is proposed and has been widely used in radio-based wireless communications. In the two-way method, two legitimate nodes send random signals to each other and use their sent and received signals to construct the common feature. In this view, the entropy of the common feature involves the channel randomness and the two-way randomness of the transmitted signal space, which thereby is able to increase the SKR as opposed to one-way and pure CSI feature-based secret keys. In the context of molecular communications, the work in [21] firstly designed a two-way based secret key generation for concentration channel, whereby Alice and Bob send binary randomness and construct the key via the sent and detected bits. However, (i) the scheme does not fully exploit the randomness of the signal space (i.e., only binary space is used), and (ii) they throw away the channel randomness by their usages of signal detection. As such, the SKR is far from reaching its limit, and can be still improved by more sophisticated signal space and feature extraction designs.

B. Real-World Demonstration of Key-based Molecular PLS

We show a demonstration of a simpler version of the molecular PLS scheme for isotropic channels where the distance estimation is used as a way to generate cipher keys - this was recently published in [25]. As shown in Table II, instead of a spectrum analyser for RF signal features, we show how to use Particle Image Velocimetry (PIV) to capture essential physics-based signal features (e.g., fluid dynamic properties) that are common between Alice and Bob. A key area of research that has not been done will be key convergence rate using a variety of co-flow channel estimation methods such as sequential Bayesian detection with random finite sets (RFS) or exploiting recent advances in deep learning to classify the common ambient vector field.

In summary, PLS in molecular communications is different compared to RF, because the biophysics propagation is different and the signal feature space is also different. In RF, we leverage on the IQ diagram (e.g., phase and magnitude) and also often using high frequency signal features. In molecular communications, we must identify new features and signal processing transforms that are robust to new channel variations (e.g., diffusion-advection currents), and because diffusion erodes high frequency signal features, we must rely on other features such as vorticity. Furthermore, the surrounding environment in RF simply acts as passive reflection or absorbing

surfaces - contributing to a multi-path and attenuation effect. On the other hand, a biological environment in molecular communications can entrap, delay, or even alter the signal through reactions and complex interactions. Even the hardware requirements for doing this are significantly different (PIV for molecular tracing and analysis instead of spectrum analyser). As such, molecular communications PLS requires both new signal processing, communication theory frameworks and new hardware.

V. Physical Asset Security: Molecular Encryption

Molecular communication leverages on diverse biochemical compounds. Some have properties which can be modulated by external forces such as temperature. To further demonstrate real lab based biochemical PLS that is unique to molecular communications, we show how security can be achieved by exploiting temperature-modulated features of protein molecules.

A. DNA-based Information with Environment-based Public Key

DNA communication is one example of structural-based molecular communication, whereby the information is modulated by the structure of molecules, other than the concentration or timing.

Encoding and modulating information on DNA strands is an emerging fundamentally new alternative to electronic and magnetic systems with orders of magnitude advantages in: durability, reliability, and high-volume data density [3], [51]. Current practices of modulating information onto DNA strands include *bar-coding* [52]. One can modulate and encode information on the DNA nano-structure at the transmitter by inserting highly conductive gold particles for 1 and leaving blanks for 0. At the receiver side, a nanopore [1] is used which consists of a pipette that draws in the DNA strand and reads its nano-structure for information. This uses a patch-clamp data acquisition technique, which includes noise cancellation signal processing and a signal feature detection algorithm (e.g., pCLAMP). The process faces challenges in attaching gold particles consistently (chemical reaction) and an optimization problem exists in the trade-off between long DNA strands (high bit/symbol) and structural shape for reliable decoding (long strands will curl making reading difficult).

Current state-of-the-art strategies rely on the encoding and decoding of long single strands in a laboratory setting, where DNA strands can be arbitrarily long. To exist in a real practical environment, DNA needs to survive inside a living host (e.g. bacteria). In such a case the long strand must be fragmented in order to fit inside bacteria without disrupting the host's functionalities. Fragmentation and re-assemble of DNA strands in the correct order opens it up for security attacks, e.g., an attacker can lure the bacteria to make the information received by legitimate receptors incomplete, and even more decode the information via its lured DNA fragments, which, however, is an area of research not currently investigated. Whilst the legitimate nodes can apply basic error correction coding ideas to deal with the incomplete fragment issue, these have a finite error detection and correction capacity and a high DNA overhead. Here, our recent research has investigated how to achieve:

- short strand DNA information bearers
- implement a common key pool, where environmental parameters that influence the molecular structure is the cipher key - see Fig. 7.

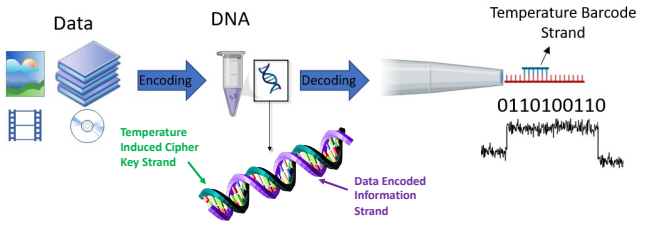

Fig. 7. Environment induced complementary DNA strands for molecular information transfer and storage in Internet-of-Nano-Things (IoNT).

In temperature-encrypted complementary short DNA complementary strands (e.g., 1 encryption DNA strand, 1 information-bearing strand), every temperature-encrypted strand will be designed so as to have different lengths and therefore hybridize in a specific location with the information-bearing strand at a specific temperature. Here is the step-by-step process:

1) The system will be optimized so that the modulated information of the information-bearing strand is read at a specific temperature (known by the decoder). The temperature variation can act as a cipher key in a common pool known to only legitimate nodes
2) After the modulated information strand is read (at the right temperature), the strand will be passed on to a high-temperature stage (above the melting temperature of the complementary strands) before reaching a sequencer where the information bearing single strand will be read.

Our system will therefore enable us to read the information stored on the DNA and assign it a unique ID. This approach is critical when trying to piece together information from various sources, but it can also be useful for additional security encoding such as considering the temperature as a layer of security to avoid eavesdropping in communication channels. The system can be optimized so that the temperature cipher code is known through the standard steps of key consolidation and secrecy maximization between transmitter and receiver.

B. Proof-of-Concept Demonstration of Micro-fluidic Protein Signal

There are a number of ways to encode molecular information in bio-molecular compounds beyond DNA/RNA strands, such as using carbohydrates and gas compounds [24]. In our novel work shown in Fig. 8a, we have demonstrated some of the possibilities using a biosensor to detect encoded Bovine Serum Albumin (BSA) protein molecules by means of a nanopore. We hypothesize that the temperature and other

[1]Nanopore is a micro-fluidic sensor that can convert certain molecular structure readings into digital signal for analysis. It is marketed and most commonly used for DNA analysis, but other molecules can also be used.

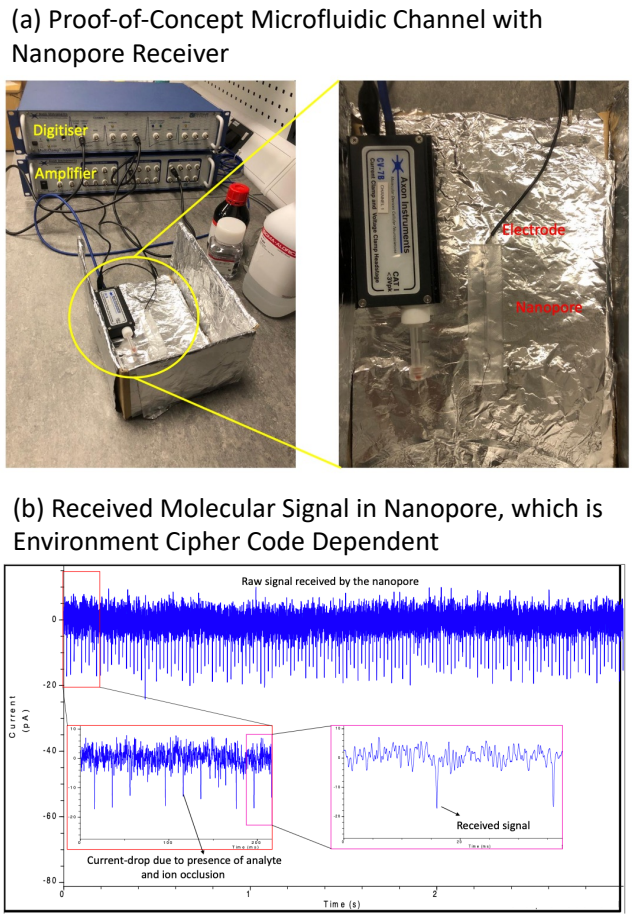

Fig. 8. Our novel Proof-of-Concept: internal micro-fluidic channel on chip is used to transfer temperature encoded protein molecules to a nano-pore analyser. The digital signal processing units are there to convert nanopore molecular communication signals into digital signals so we can verify the findings. The subplots are: (a) micro-fluidic chip with (b) encrypted BSA protein molecule signal detection using nanopore sensing presents the potential of environment-based encoding.

environmental conditions will affect both the modulated and detected signal and therefore act as a common key.

The proof-of-concept setup in Fig. 8a consists of a fabricated glass micro-fluidic channel with a reservoir, pump, electrolyte carriers, and nanopore sensing. The receiver is a Digi-data 1550B digitizer with MultiClamp 700B amplifier with pClamp detection software to record the acquired BSA protein signal. In principle, nanopore works based on simple resistive pulses, and the molecules can be detected by the exclusion of ions when they go through a nanoscale channel. From the shape of an individual protein detection event, information about the physical and chemical properties of the protein molecule can be inferred (e.g., in Fig. 8b temperature at transmitter acts as an encoding cipher), which correlates with the initial environmental conditions at the transmitter, and hence provide a form of environment-based security. Our initial laboratory results pave the way for future work on encoding and decoding DNA molecules.

VI. Conclusions & Future Work

Here, in this novel review, we showed that new vectors of attack and new methods to achieve molecular information security are emerging. This review examined recent work spanning the secrecy information rate of molecular channels, using environmental conditions as cipher keys, to how to encode data using unique sparse signal patterns. Much more work is needed in this space, not only because of its cross-disciplinary nature, but also because building the first experiments in IoNT security takes time and significant funding. The maturity of this work is currently at Technology Readiness Level (TRL) 2-4, and we have shown 2 of our novel proof-of-concept demonstrations by our lab [9]. We have also reviewed the work by others around the world [3] [24] in this paper. In almost all our work, there is a direct experimental platform or a connection to one. The work leverages more established synthetic biology and cybersecurity research to bring about innovation for molecular IoNT.

Future work directions are exciting and require combined efforts from information theory, network science, cybersecurity, and bio-engineering research to build real IoNT systems that tackle 3 main research areas: (1) better analysis of the secure information capacity of complex fluid dynamic channels representative of in-vivo environments (e.g., conditional mutual information of Reynolds Averaged Navier-Stokes dynamics), (2) embed security-by-design in the molecular properties to achieve biochemical information security, and (3) create robust ad-hoc molecular IoNT network protocols that are lightweight. I believe these contribute towards emerging standards such as P1906 and future 6G wireless systems [9], [53].

Contributions: S.Q. and W.G. developed the idea of the paper. Z.W., Y.H. and W.G. reviewed and tested the key-less and key-based PLS for molecular communications. M.A. and J.C. did the simulation and hardware experiments of protein-based molecular encryption. B.L. and Y.H. provided guidance on different models (concentration and timing) of molecular communications. B.L. provided guidance on numerical optimizations. W.G. and B.L. provided guidance on the problem context and impact pathway. S.Q., Z.W. and W.G. wrote the paper.

Conflicts of Interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. Canovas-Carrasco, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "The ieee 1906.1 standard: Nanocommunications as a new source of data," *in 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, pp. 1–7, 2017.

[2] I. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The Internet of Bio-Nano things," *IEEE Communications Magazine*, vol. 53, no. 3, Mar. 2015.

[3] N. Goldman, P. Bertone, S. Chen, C. Dessimoz, E. LeProust, B. Sipos, and E. Birney, "Towards practical, high-capacity, low-maintenance information storage in synthesized DNA," *Nature Nanotechnology*, vol. 494, pp. 645–651, 2013.

[4] S. M. Abd El-atty and A. Tolba, "A cross-layer approach for optimization of molcom systems toward the internet of bio-nanothings," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2751–2762, 2019.

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

[6] Y. Wang, M. Guo, B. He, and B. Gao, "Intelligent patches for wound management: In situ sensing and treatment," *ACS Anal. Chem.*, vol. 93, no. 11, p. 4687–4696, Mar 2021.

[7] B.-B. C. Youan, "Chronopharmaceutical drug delivery systems: Hurdles, hype or hope?" *Advanced Drug Delivery Reviews*, vol. 62, no. 9, pp. 898 – 903, 2010.

[8] S. Kumar, "Nanomachine localization in a diffusive molecular communication system," *IEEE Systems Journal*, vol. 14, no. 2, 2020.

[9] W. Guo, M. Abbaszadeh, L. Lin, J. Charmet, P. Thomas, Z. Wei, B. Li, and C. Zhao, "Molecular Physical Layer for 6G in Wave-Denied Environments," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 33–39, 2021.

[10] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[11] 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*, 2023.

[12] F. Dresler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Communication Networks*, vol. 3, no. 3, 2012.

[13] 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*, 2021.

[14] 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, 2019.

[15] 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, Sep. 2016.

[16] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Transactions on NanoBioscience*, vol. 13, 2014.

[17] K. Yang, D. Bi, Y. Deng, R. Zhang, M. M. U. Rahman, N. A. Ali, M. A. Imran, J. M. Jornet, Q. H. Abbasi, and A. Alomainy, "A comprehensive survey on hybrid communication in context of molecular communication and terahertz communication for body-centric nanonetworks," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 2, pp. 107–133, 2020.

[18] S. P. Singh, S. Yadav, R. K. Singh, V. Kansal, and G. Singh, "Secrecy capacity of diffusive molecular communication under different deployments," *IEEE Access*, vol. 10, pp. 21 670–21 683, 2022.

[19] S. Riazul Islam, F. Ali, H. Moon, and K.-S. Kwak, "Secure channel for molecular communications," in *International Conference on Information and Communication Technology Convergence*, 2017.

[20] Q. Liu, P. He, K. Yang, and S. Leng, "Inter-symbol interference analysis of synaptic channel in molecular communications," in *IEEE International Conference on Communications (ICC)*, 2014.

[21] S. M. R. Islam, F. Ali, H. Moon, and K. Kwak, "Secure channel for molecular communications," in *International Conference on Information and Communication Technology Convergence*, Oct 2017.

[22] G. Sharma and A. Singh, "Secrecy loss in diffusive molecular timing channels," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2022.

[23] 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.

[24] D. T. McGuiness, S. Giannoukos, A. Marshall, and S. Taylor, "Experimental results on the open-air transmission of macro-molecular communication using membrane inlet mass spectrometry," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2567–2570, Dec 2018.

[25] W. Guo, Z. Wei, and B. Li, "Secure internet-of-nano things for targeted drug delivery: Distance-based molecular cipher keys," in *IEEE 5th Middle East and Africa Conference on Biomedical Engineering*, 2020.

[26] V. Jamali, A. Ahmadzadeh, W. Wicke, A. Noel, and R. Schober, "Channel modeling for diffusive molecular communication?a tutorial review," *Proceedings of the IEEE*, vol. 107, July 2019.

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

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

[29] N. Farsad, D. Pan, and A. Goldsmith, "A novel experimental platform for in-vessel multi-chemical molecular communications," in *IEEE Global Communications Conference*, Dec 2017.

[30] S. Qiu, W. Haselmayr, B. Li, C. Zhao, and W. Guo, "Bacterial relay for energy-efficient molecular communications," *IEEE Transactions on NanoBioscience*, vol. 16, no. 7, pp. 555–562, 2017.

[31] L. Katharina, S. Jon, T. Shane, A. Jalal, B. M. Nahom, H. A. Maynard, K. Raza, and L. Karen, "How to analyze the cyber threat from drones," *RAND Report RR2972; RAND Corp.: Santa Monica, CA, USA*, 2020.

[32] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 665–676, 2016.

[33] A. Etemadi, M. Farahnak-Ghazani, H. Arjmandi, M. Mirmohseni, and M. Nasiri-Kenari, "Abnormality detection and localization schemes using molecular communication systems: A survey," *IEEE Access*, vol. 11, pp. 1761–1792, 2023.

[34] M. Schurwanz, P. A. Hoeher, S. Bhattacharjee, M. Damrath, L. Stratmann, and F. Dressler, "Duality between coronavirus transmission and air-based macroscopic molecular communication," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 7, no. 3, pp. 200–208, 2021.

[35] M. Abbaszadeh, P. J. Thomas, and W. Guo, "Toward high capacity molecular communications using sequential vortex rings," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 4, no. 1, pp. 39–42, 2018.

[36] P. Rojas, S. Alahmadi, and M. Bayoumi, "Physical layer security for iot communications - a survey," in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 2021, pp. 95–100.

[37] X. Zhang and E. W. Knightly, "$csisnoop$: Inferring channel state information in multi-user mimo wlans," *IEEE/ACM Transactions on Networking*, vol. 27, no. 1, pp. 231–244, 2019.

[38] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, "Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1831–1845, 2020.

[39] F. Vakilipoor, A. N. M. Ansari, and M. Magarini, "Localizing the unknown receiver in a diffusive simo molecular communication system," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 9, no. 1, pp. 18–22, 2023.

[40] G. Sharma, N. Pandey, A. Singh, and R. K. Mallik, "Security in diffusive molecular timing channels: An amount of confusion level perspective," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2022.

[41] S. Wang, L. Peng, H. Fu, A. Hu, and X. Zhou, "A convolutional neural network-based rf fingerprinting identification scheme for mobile phones," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 115–120.

[42] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, 2017.

[43] V. Jamali, A. Ahmadzadeh, W. Wicke, A. Noel, and R. Schober, "Channel modeling for diffusive molecular communication—a tutorial review," *Proceedings of the IEEE*, vol. 107, no. 7, pp. 1256–1301, 2019.

[44] M. Abbaszadeh, I. U. Atthanayake, P. J. Thomas, and W. Guo, "Molecular signal tracking and detection methods in fluid dynamic channels," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 2, pp. 151–159, 2020.

[45] S. Zafar, W. Aman, M. M. U. Rahman, A. Alomainy, and Q. H. Abbasi, "Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system," in *2019 UK/ China Emerging Technologies (UCET)*, 2019, pp. 1–2.

[46] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, 2016.

[47] Z. Wei, W. Guo, B. Li, J. Charmet, and C. Zhao, "High-dimensional metric combining for non-coherent molecular signal detection," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1479–1493, 2020.

[48] A. Noel, K. C. Cheung, and R. Schober, "Joint channel parameter estimation via diffusive molecular communication," *IEEE Transactions*

on Molecular, Biological and Multi-Scale Communications, vol. 1, no. 1, pp. 4–17, 2015.

[49] L. Lin, C. Yang, S. Ma, and M. Ma, "Parameter estimation of inverse gaussian channel for diffusion-based molecular communication," in *2016 IEEE Wireless Communications and Networking Conference*, 2016.

[50] B. Li, M. Sun, S. Wang, W. Guo, and C. Zhao, "Local Convexity Inspired Low-complexity Non-coherent Signal Detector for Nano-scale Molecular Communications," *IEEE Transactions on Communications*, vol. 64, Jan. 2016.

[51] M. E. Ortiz and D. Endy, "Engineered cell-cell communication via dna messaging," *Journal of Biological Engineering*, vol. 6, 2012.

[52] N. Bell and U. Keyser, "Digitally Encoded DNA Nanostructures for Multiplexed, Single-Molecule Protein Sensing with Nanopores," *Nature Nanotechnology*, vol. 11, 2016.

[53] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6g technologies and applications," *Sensors*, vol. 22, no. 5, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/5/1969