

A Review of Confidentiality, Integrity, and Availability Challenges in Molecular Communications

Malcolm I. Anderson *Student Member, IEEE*, Truc T. Duong *Student Member, IEEE*, Ebuka P. Oguchi *Member, IEEE*, Anna Wisniewska *Member, IEEE*, Nirimesh Ghose *Senior Member, IEEE*

Abstract—Molecular communications (MC) are emerging paradigms that aim to transform communication at the micro- and nanoscale levels by utilizing molecules as information carriers. Unlike traditional communication, molecular communication uses chemical signals, which provide distinct advantages in biological contexts. This review examines important advances in molecular communication security customized for these unique communication channels. We highlight risks and challenges in molecular systems, focusing on the confidentiality, integrity, and availability security objectives that are critical for applications such as targeted drug delivery (TDD) and in vivo networks. Furthermore, we discuss potential attacks, interdisciplinary security measures, physical/MAC layer strategies, and hybrid networks. Our contributions provide a complete overview of existing research, identify critical challenges, and potential solutions to ensure secure and reliable molecular communication.

Index Terms—Molecular communication, bio-nanomachines, confidentiality, integrity, availability, information theoretic bounds, secrecy capacity.

I. INTRODUCTION

MOLECULAR communication (MC), and the Internet of Bio-Nano Things (IoBNT) are emerging paradigms enabling communication between nano-scale devices or within biological systems [1]–[3]. In molecular communication, information is transmitted by encoding it into the properties or distribution of molecules, allowing communication among biological cells, organisms, or nano-scale devices. Molecules are released into mediums such as water, air, or biological fluids, with information encoded in molecular concentration [4], [5], type [6], or release timing [7], [8]. These encoded molecules propagate through the medium to deliver information to a receiver. Molecular communication has been extensively applied in nanotechnology, synthetic biology, and biomedicine. Applications include targeted drug delivery [9]–[11], environmental monitoring [12], and hybrid communication between synthetic and biological systems [9]. These advances demonstrate the significant potential of molecular communication in addressing real-world challenges across various domains.

The Internet of Bio-Nano Things (IoBNT) extends the Internet of Things (IoT) paradigm by integrating nanoscale

devices and biological components into the IoT ecosystem. IoBNT facilitates seamless communication, data exchange, and control between bio-nano devices, nano-machines, biological systems, and conventional IoT devices through molecular communication technique [13]. Although molecular communication and IoBNT are primarily designed for nano-scale operations, they often function at the micro-scale. In molecular communication, information-carrying molecules interact with micro-scale biological structures such as cells, tissues, or microfluidic channels. Similarly, IoBNT applications may involve communication at the micro-scale, enabling interactions between embedded micro-scale sensors, actuators, and devices in biological systems, bridging the gap between nano- and macro-scale systems.

Ensuring security in molecular communication channels presents unique challenges and opportunities, from mitigating signal interference and molecular noise to safeguarding against eavesdropping and tampering. Robust security measures are essential to foster trust and reliability in molecular communication infrastructures [10], [14], [15]. According to the National Institute of Standards and Technology (NIST), confidentiality, integrity, and availability (CIA) are the most critical security objectives to ensure secure communication [16]. Traditional electromagnetic (EM) communication systems have well-established data protection algorithms that guarantee confidentiality [17], integrity [18], and privacy [19]. However, these methods cannot be directly transferred to molecular communication due to the unique constraints of these systems, such as limited computational capabilities, energy constraints, and physical properties of the communication medium [20].

The focus has primarily been on the physical layer of MC networks, investigating signal propagation, noise analysis, and channel capacity [21]–[26]. Although this has advanced the reliability of molecular communication, it has not fully addressed the security implications. Current methods lack tailored approaches to ensure confidentiality, integrity, and availability in critical components to secure communication involving sensitive data, such as in healthcare, targeted drug delivery, and environmental monitoring. In these situations, lack of security could have disastrous consequences, including unauthorized dosage changes, disclosure of personal health data, and interference with living organism medical protocols.

In this paper, we focus on the confidentiality, integrity, and availability security objectives to synthesize state-of-the-art security approaches in MC. We review attack vectors in

Malcolm I. Anderson, Truc T. Duong, and Anna Wisniewska are with the Department of Computer Science, Washington State University Vancouver, USA (e-mail: {malcolm.i.anderson, truc.duong, anna.wisniewska}@wsu.edu). Ebuka P. Oguchi is with the Department of Computer and Information Sciences, Spelman College (e-mail: ebukaoguchi@spelman.edu). Nirimesh Ghose is with the School of Computing, University of Nebraska–Lincoln (e-mail: nghose@unl.edu). Malcolm I. Anderson, Truc T. Duong, and Ebuka P. Oguchi contributed equally to this work.

Manuscript received January XX, 20XX; revised May XX, 20XX.

detail, e.g., eavesdropping, jamming, spoofing, and denial of service, to understand how information molecules (IMs) can be transmitted reliably and securely. Recognizing that this is a highly interdisciplinary area that takes inspiration from fields including computer science, biochemistry, neuroscience, and biology, we investigate research across fields to determine how they contribute to the development of MC networks. Furthermore, we look at hybrid networks that may enhance security by allowing the unique characteristics of MC to complement those of traditional electromagnetic networks.

We contribute to existing reviews by (1) focusing on the CIA triad, (2) providing an extensive overview of attack vectors, (3) stressing interdisciplinary solutions, (4) exploring approaches for the physical/MAC layers, and (5) discussing the interface between MC and EM networks (i.e., hybrid networks). Many surveys on molecular communication acknowledged security as an important area, but have limited discussion of the security implications in these networks [14], [27]–[30]. For the purposes of systematically addressing security concerns in MC, a comprehensive list of attack vectors is crucial. Existing surveys focus only on a subset of attacks and the corresponding solutions [31], [32]. In [33], [34], security challenges and solutions for the physical layer are reviewed. Here, protocols and security strategies are reviewed both in the physical layer and in the MAC layer for a holistic view of security implications. In [35], [36], the focus is on security for bio-cyber interfaces and hybrid networks, which utilize both EM and MC technologies, while in contrast, our focus is on security in MC networks.

Paper Organization: In Section II, attack vectors in molecular communication are discussed. In Section III, security solutions organized using the security objectives confidentiality, integrity, and availability are reviewed. In Section IV, gaps and potential future directions are identified. Finally, we conclude the paper in Section V.

II. CYBERSECURITY VULNERABILITIES

Addressing threats such as eavesdropping, denial of service, spoofing, and jamming attacks ensures the reliability of information molecules transmitted by a biological cell or material. In this section, we present an overview of various cyber attacks and their effects on molecular communication. Figures 1-5 illustrate the flow of molecules from a legitimate transmitter (Alice) to a legitimate receiver (Bob), while capturing the influence of either a passive adversary (Eve) or an active adversary (Mallory).

A. Attack Compromising Confidentiality

1) *Eavesdropping:* Malicious devices can intercept information molecules as they diffuse through the medium toward their intended recipient [37], harming system confidentiality. If MC signals propagate in the direction of a malicious device, the attacker can eavesdrop on the transmitted message. This issue is especially critical in diffusion- and flow-based MC systems, where IMs are freely broadcast throughout the medium to maximize the likelihood of message delivery. Broadcasting inadvertently increases the risk of interception by malicious entities [33], [38]–[40].

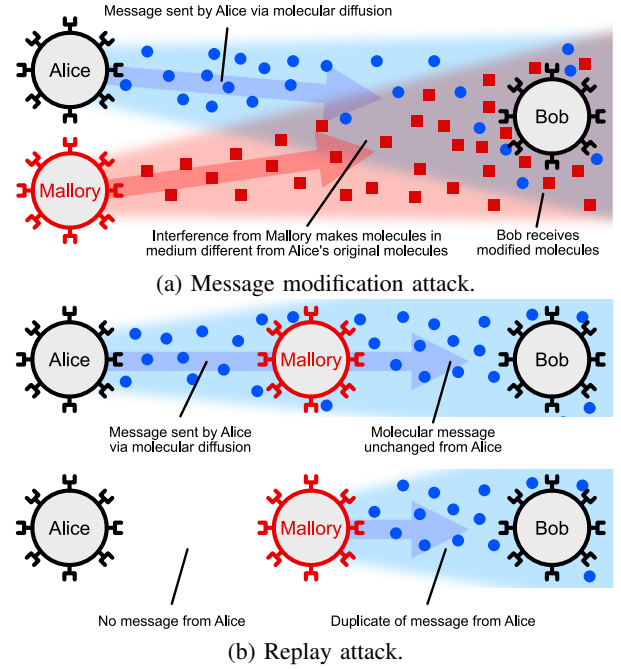


Fig. 1: Attacks that compromise integrity.

B. Attacks Compromising Integrity

1) *Message Modification Attack:* In molecular communication networks, the limited communication range of nano-devices often necessitates multi-hop transmission, where messages pass through multiple intermediary nodes to reach their intended destination. Multi-hop architecture introduces vulnerability to message modification attacks, as shown in Fig. 1a. Malicious nodes between the sender and the receiver can intercept the transmitted message, alter its content, and relay the modified version [41]. Interference of this type can lead to unintended and potentially harmful outcomes, e.g., issuing false commands to trigger actions such as premature release of medicine in healthcare applications [29]. Addressing this threat requires robust integrity verification mechanisms and secure routing protocols designed for the unique constraints of molecular communication networks.

2) *Replay Attack:* Malicious nano-devices can exploit previously intercepted messages through eavesdropping to perform replay attacks, as shown in Fig. 1b. By capturing legitimate commands from authorized devices, attackers can resend these messages repeatedly to disrupt system functionality [42]. To launch a replay attack in molecular communication, an adversary records the time-series molecular distribution and retransmits an amplified replica to compensate for channel attenuation; however, variations in environmental conditions significantly complicate accurate replay, increasing the difficulty for the attacker. Replay attacks can trigger the unintended and repetitive release of drugs in healthcare applications, potentially leading to overdoses or other severe consequences. To mitigate these threats, molecular communication networks must implement robust countermeasures, such as timestamps and nonce-based mechanisms [41], to ensure the uniqueness and validity of each transmitted command. These solutions are essential to safeguard against unauthorized retransmissions in these sensitive networks. Frequently in MC, receivers absorb

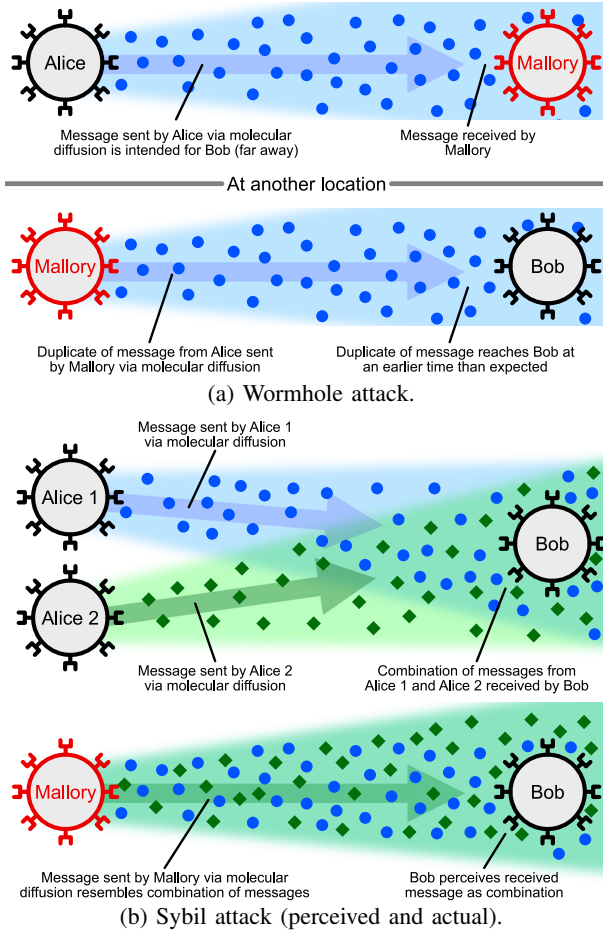


Fig. 2: Attacks that compromise integrity.

IMs for the purpose of reducing the remaining noise in the channel [43]. If done by an unauthorized third party, this hinders the availability of messages for the intended recipients.

3) **Wormhole Attack:** An attacker can create network wormholes by relaying messages between distant nodes, bypassing established communication pathways, as shown in Fig. 2a. These attacks compromise the integrity, confidentiality, and reliability of the communication network, making the development of robust routing protocols and secure authentication mechanisms critical to mitigate such vulnerabilities [44]. A wormhole attack in molecular communications, analogous to a replay attack, can be realized by recording the time-series molecular distribution near the transmitter and releasing an amplified version of the same type of molecule closer to the receiver. However, executing a wormhole attack poses substantial practical challenges. The adversary must possess the capability to synthesize and emit identical molecules, and the environmental conditions near the transmitter may differ significantly from those near the receiver. These mismatches can severely complicate signal reproduction and propagation, thereby exacerbating the logistical complexity and making wormhole attacks difficult to carry out in molecular communication networks.

4) **Sybil Attack:** An attacker can deploy multiple fake identities within the network to manipulate communication or gain unauthorized access to the system, as shown in Fig. 2b. These counterfeit identities can disrupt network

operations by propagating misleading data, causing network congestion, or undermining trust-based protocols [32], [36]. A Sybil attack in molecular communication can be realized when an adversary injects multiple distinct molecular identity signatures into the channel to impersonate several legitimate transmitters simultaneously. By carefully releasing different molecule types or temporal emission patterns associated with unique identities, the attacker attempts to create the illusion of multiple independent nodes. However, executing a Sybil attack is non-trivial in molecular environments. The adversary must generate and coordinate multiple distinguishable molecular signatures while accounting for diffusion, environmental noise, and inter-symbol interference. Furthermore, spatio-temporal correlations in molecular propagation may reveal inconsistencies among the forged identities, thereby complicating the attack and making reliable Sybil impersonation challenging in molecular communication networks.

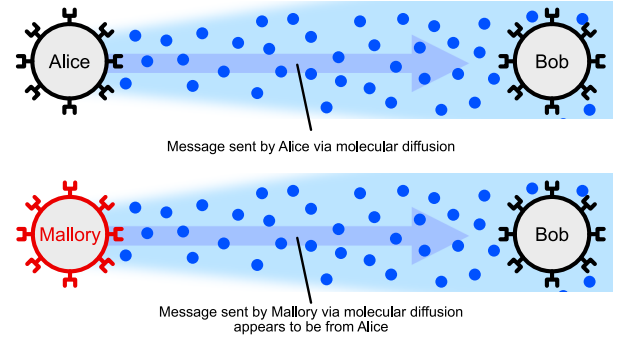


Fig. 3: Impersonation attack that compromises integrity.

5) **Impersonation Attack:** Unauthorized nano-machines can mimic legitimate devices within the network, gaining access to critical data or disrupting operations, as shown in Fig. 3. Impersonation attacks pose significant security risks, particularly in systems where accurate device identification is vital [45]. In healthcare networks, an attacker could impersonate a valid medical nano-machine, gaining access to sensitive patient information or issuing harmful commands [46]. An adversary may record the molecular distribution transmitted by a legitimate transmitter, including the molecular type encoding the identity signature; however, temporal variations in environmental conditions significantly complicate reproducing an identical molecular distribution at the receiver, making successful identity impersonation difficult.

C. Attacks Compromising Availability

1) **Jamming Attack:** A jamming attack in molecular communication can be realized by introducing molecular inhibitors that obstruct signal propagation or by releasing neutralizing molecules that chemically eliminate information molecules from the channel, as shown in Fig. 4. The signal-to-noise ratio (SNR) for MC channels is often lower than that of traditional EM communication channels due to factors such as Brownian motion within the transmission medium [47]. Jamming attacks further degrade the signal-to-noise ratio, making it difficult for receivers to interpret the intended messages accurately [48], [49]. Such attacks are particularly detrimental for life-critical systems, where precise molecular communication is essential for triggering medical responses or managing autonomous

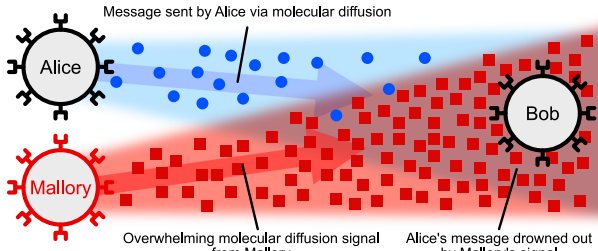


Fig. 4: Jamming attack that compromises availability.

nano-machines. Disrupted communication could result in delayed or incorrect therapeutic actions, potentially leading to severe consequences for patient safety and system reliability. Robust noise mitigation and interference detection techniques are critical to effectively counteract these threats [50]–[52].

2) *Blackhole Attack*: Malicious bio-nanomachines can deploy chemo-attractants to lure legitimate nano-machines toward themselves [53], [54], as shown in Fig. 5a. A blackhole attack in molecular communication occurs when a malicious node releases attracting molecules along the propagation path, drawing information molecules away from the intended receiver, and thereby disrupting communication at the target location while diverting it toward an alternate location. A malicious node need not be co-located with the intended receiver; it may be deployed anywhere along the propagation path, provided it can still pull information molecules away from their intended destination. In a targeted drug-delivery scenario, a malicious blackhole node may release chemo-attractants that pull therapeutic information molecules away from the diseased tissue, thereby reducing delivery to the intended target and potentially causing off-target accumulation elsewhere. Additionally, for early disease-detection, a malicious blackhole node can attract biomarker-carrying information molecules away from the sensing region. This tactic disrupts the communication flow by diverting information molecules from their intended trajectories, which is particularly detrimental given the limited communication range of these devices. Such diversion can prevent legitimate nano-machines from performing essential tasks. Chemo-attractants may also interfere with other processes within the medium. For example, in biological environments such as the human body, malicious attractants could lure lymphocytes away from infection sites, weakening the immune system's ability to suppress harmful pathogens [55].

3) *Sentry Attack*: Malicious nano-devices can deploy chemo-repellents to prevent legitimate nano-machines from reaching their intended destinations [53], [54], as shown in Fig. 5b. A sentry attack in MC occurs when a malicious node releases repelling molecules that divert information molecules away from their intended receiver toward an alternate location, thereby altering the effective communication path. A malicious node can be deployed anywhere along the propagation path, provided that it can deflect information molecules away from their intended destination. In a targeted drug-delivery system, a malicious sentry node may release chemo-repellent molecules that deflect therapeutic information molecules away from the diseased tissue, thus delaying delivery or preventing the

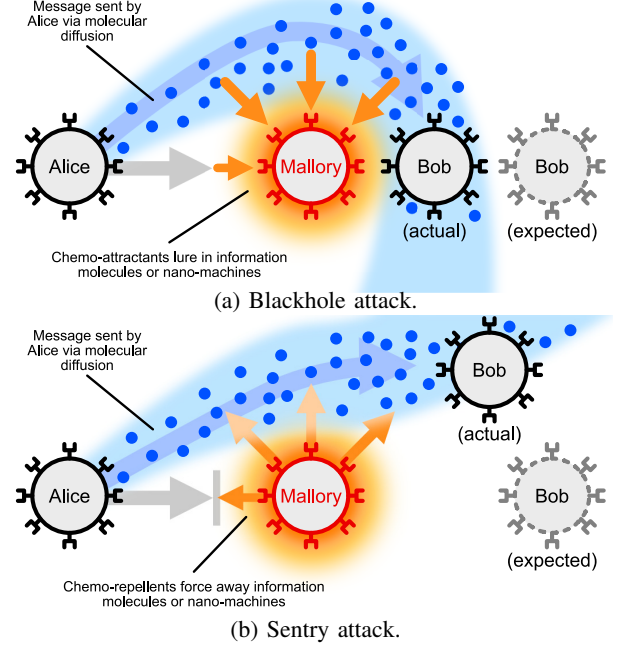


Fig. 5: Attacks that compromise availability.

required dose from reaching the intended target. Additionally, in an immune-signaling coordination scenario, a sentry node can release chemo-repellent molecules that divert signaling molecules away from their intended immune cells, thereby weakening the coordinated response at the infection site. This tactic can hinder legitimate devices from performing essential tasks, such as drug delivery and the detection of abnormalities caused by malicious nano-devices. By delaying or preventing legitimate nano-machines from sensing and responding to abnormal behavior, chemo-repellent attacks can amplify the damage caused by other malicious entities within the network. Furthermore, sentry attacks can have consequences beyond the nano-communication system itself. For instance, chemo-repellents could disrupt the interaction between specific organisms and environmental chemicals, thereby impeding processes such as pollutant degradation. In such cases, chemical treatments designed to mitigate environmental damage may become ineffective, leading to long-term ecological harm [55].

III. CYBERSECURITY SOLUTIONS

In this section, an overview of existing solutions for the confidentiality, integrity, and availability vulnerabilities discussed in the previous section is presented.

A. Confidentiality

Molecular communication security literature has primarily focused on ensuring confidentiality and privacy [19], [37], [40], [56]–[59]. Confidentiality protects information molecules from being accessed by unintended entities. In contrast, privacy ensures that the identities and actions of nano-machines remain undisclosed. Molecular communication differs from conventional electromagnetic systems since signal propagation is based on stochastic biochemical processes, such as diffusion, degradation, flow, and receptor binding, making confidentiality attacks highly dependent on the environment and propagation medium. These uncertainties complicate the detection of eavesdropping and limit the effectiveness of conventional

cryptographic techniques due to the resource constraints of nanomachines, motivating alternative confidentiality mechanisms based on information-theoretic limits, molecular timing, and cooperative communication.

In MC, a confidentiality attack is not merely a passive interception of propagated signals; rather, it is an environment-dependent biochemical inference task where successful interception depends on molecular transport, degradation, and the attacker's ability to achieve compatible molecular recognition [60]. Eavesdropping in MC not only compromises confidentiality, it may also reveal signaling patterns, timing information, and control commands that enable later reply, impersonation, or message-modification attacks. Unlike attacks in EM communication where the protocol and frequency are known, MC confidentiality attacks require target-specific synthetic receptors, probes, or engineered cells, making them difficult to replicate across biochemical environments [61]. If a system uses engineered cells, synthetic ligands, or custom receptor pathways, an attacker may need to engineer a compatible biological interface to intercept or decode the message. This requirement makes such attacks difficult to generalize across different targets. An interception mechanism designed for one ligand-receptor pair, one yeast signaling circuit, or one soluble factor may not be applicable to other target types without substantial redesign. Recent studies on synthetic cells and engineered yeast show that communication behavior depends strongly on the specific design of the underlying signaling pathways [61]–[65].

Environmental effects make confidentiality attacks difficult to replicate. Temperature, viscosity, flow, heterogeneous boundaries, crowding, and degradation alter arrival times and concentration profiles. Therefore, an adversary (Eve) may observe different signal statistics in different environments. In other words, the environment not only reduces reliability for the receiver (Bob), but also introduces uncertainty into Eve's attack. Thus, the same eavesdropping strategy may work in one tissue or fluid environment, while it fails in another, since the channel itself changes [66]. Various strategies for achieving confidentiality and privacy, categorized into information-theoretic bounds, diffusive molecular timing, and multi-node communication, are discussed next.

1) *Information Theoretic Bounds*: Understanding MC systems requires the application of information theory to establish theoretical bounds on performance metrics, e.g., channel capacity, mutual information, and secrecy capacity [67]. Consequently, secrecy in MC depends not only on the signal strength but also on biochemical compatibility, environmental variability, and the attacker's ability to recognize or reproduce the correct molecular signatures. These limits are critical for designing efficient and secure communication protocols, especially in complex environments such as biological systems. In contrast to EM systems, where eavesdropping is often modeled as passive signal capture, confidentiality attacks in MC are constrained by uncertain molecular propagation, degradation, and biochemical specificity.

Channel capacity defines the maximum information transfer rate that a communication channel can reliably support. For MC systems, this depends on factors such as diffusion rates,

molecular degradation, distance, and environmental conditions [40]. For instance, in diffusion-based systems, channel capacity is constrained by stochastic molecular propagation and inter-symbol interference (ISI). Theoretical expressions for channel capacity have been extensively developed and studied [37], [68]. These formulations help characterize and improve communication efficiency in MC systems.

Mutual information quantifies the information shared between a transmitted signal and the received signal, accounting for the stochastic nature of diffusion and environmental noise [40]. Despite unpredictable diffusion dynamics, this metric evaluates how accurately information molecules convey meaningful data. Mutual information has been analyzed to optimize MC system designs for reliable communication in noisy environments [68]. In addition to diffusion noise, factors such as degradation, competing reactions, crowding, and local concentration fluctuations affect the signal and, consequently, the amount of information available to an eavesdropper. However, an adversary equipped with engineered receptors or chemically selective probes may partially compensate for weak signal strengths. This distinguishes MC from EM systems, where front-end receivers generally do not require biochemical redesign for each target environment.

Secrecy capacity represents the maximum secure data transmission rate between two parties (Alice and Bob) while ensuring that Eve cannot decode the intercepted data. Various techniques, including chemical camouflage and receptor-specific targeting, have been proposed to enhance secrecy in MC. Stochastic models for molecule absorption and ISI provide insight into vulnerabilities and solutions to secrecy [40]. Secrecy capacity is influenced by molecular absorption, degradation, ligand-receptor affinity, and intersymbol interference, and can be enhanced through approaches such as chemical camouflage, artificial interference molecules, and receptor-specific signaling [40]. Since MC attacks are often target- and chemistry-specific, requiring engineered receptors or compatible molecular interfaces, they are less transferable than attacks in EM systems. Most existing analyses rely on idealized diffusion models that may not fully capture realistic biochemical interactions and environmental variability.

2) *Diffusive Molecular Timing (DMT)*: Confidentiality and privacy techniques, such as diffusive molecular timing, enhance secrecy against eavesdropping and replay attacks by introducing randomization and obfuscation that hinder adversarial inference. This creates temporal uncertainty that can hinder eavesdropping and replay attacks. For replay-related confidentiality leakage, stochastic timing and channel memory complicate the inference of release patterns from intercepted signals. Sharma *et al.* proposed methods to improve secrecy in DMT channels [56] and analyzed the effects of an interferer and an eavesdropper (Eve) on secrecy performance. Introducing an interference node into the Alice-Eve communication link can create confusion for Eve, thereby enhancing secrecy in noise-limited and interference-limited environments.

3) *Multi-Node Communication*: MC security literature has focused on single-transmitter, single-receiver systems with a single eavesdropper [37], [56], [59], [69]. However, real-world MC often involves multiple transmitters and receivers. Sabu

et al. explored communication between a single transmitter and multiple fully absorbent receivers in a 3D medium [57]. Similarly, Huang *et al.* characterized communication between a single transmitter and two absorbing receivers in a 1D medium [70]. However, both studies omitted the presence of eavesdroppers, leaving a gap in the understanding of security implications in multi-node scenarios.

In multi-node MC systems, confidentiality threats are compounded by the need for an adversary to intercept and disentangle multiple signals amid stochastic diffusion, degradation, drift, and receptor competition, which can naturally obscure target transmissions. Although a sophisticated attacker may deploy multiple engineered receptors to distinguish links, these target-specific biochemical customization limits attack generalization, leaving confidentiality in large-scale MC networks underexplored—especially under realistic environmental variability and coordinated adversarial settings [71]–[73]. Current confidentiality and privacy solutions in molecular communication provide valuable theoretical insights, but often rely on simplified models and limited adversarial assumptions. In practice, environmental heterogeneity, biochemical interactions, and target-specific receptor requirements strongly influence the feasibility and scalability of attacks. Consequently, MC confidentiality can be highly environment-dependent compared with EM, highlighting the need for more realistic and scalable security models.

B. Integrity

Integrity verification in MC is critical to ensure the correctness and reliability of transmitted data. Nano-machines have limited computational power and memory, while stochastic propagation effects such as Brownian motion, viscosity, and temperature introduce delays and variability that are less prominent in EM systems, limiting the applicability of conventional cryptographic methods [47], [74]. These issues are especially critical in medical applications, where communication must not disrupt natural biological processes, as interference could adversely affect therapies such as targeted drug delivery [75]. Next, an overview of strategies for achieving data integrity is presented, categorized into error correction, lightweight coding methods, and machine learning applications, followed by an overview of authentication methods.

1) *Error Detection and Correction Techniques:* Error correction and detection techniques ensure data integrity in MC systems. These methods enable the identification and correction of errors introduced by noisy channels or malicious interference. Deoxyribonucleic acid (DNA) stores genetic information. Naturally occurring error correction mechanisms help repair DNA damage and reduce the accumulation of mutations [76]. The established role of DNA as an information-carrying molecule, its compatibility with biological mediums, and its resilience to molecular damage make it a compelling medium for data transmission in molecular networks. Erlich *et al.* introduced DNA Fountain, a coding-theoretic approach capable of storing complex datasets, such as an operating system and a movie, in DNA oligonucleotides [77]. This approach enables accurate data retrieval with minimal sequencing coverage. Similarly, Zhang *et al.* proposed a hybrid encoding scheme that

combined minimal Hamming distance and multiple sequence alignment to address sequence defects [78].

2) *Lightweight Channel Coding:* Lightweight coding techniques are essential in molecular communication systems, since bio-nanodevices have constrained energy, memory, and processing capacity. Lightweight coding techniques mitigate issues like inter-symbol interference while remaining computationally efficient. For example, Jing *et al.* proposed a lightweight channel coding scheme to mitigate ISI in biosensor networks [79]. By avoiding consecutive and trailing 1-bits, the scheme reduces molecular accumulation within the channel, improving the bit error rate (BER). Its simplicity and low time complexity make it suitable for resource-constrained nano-devices. Tang *et al.* combined Reed-Solomon error correction codes with probabilistic constellation shaping (PCS) to optimize diffusion-based MC [80]. Their scheme uses molecular shell mapping to reduce energy consumption while mitigating ISI. Integrating error correction with PCS improved BER and robustness, despite resource constraints and channel variability.

3) *Machine Learning Applications:* A major challenge in MC compared with traditional EM communication systems is that MC faces greater variability in the communication medium. Numerous factors can affect communication and potentially corrupt the intended molecular signal, compromising integrity. Given the complexity and variability of these factors, designing protocols that account for all of them may be impractical. Machine learning (ML) techniques offer a promising approach to these challenges by detecting how channel conditions affect signals and by correcting them to maintain message integrity. Leveraging ML models for nano-receivers can mitigate channel imperfections and reduce ISI. Kim *et al.* proposed the concentration-shifted key position (CSKP) modulation scheme for molecular communication [81]. CSKP integrates a classification-based machine learning model at the nano-receiver, enabling it to outperform conventional maximum likelihood receivers. The ML model effectively learns and compensates for channel bias caused by MC channel-specific factors such as diffusion, improving communication reliability. Scazzoli *et al.* propose a data-augmentation approach for molecular communication that generates synthetic datasets from limited real measurements, enabling effective training of machine-learning models [82]. By incorporating channel effects such as saturation and impulse-response interactions, synthetic data significantly improve the decoding accuracy based on convolutional neural networks (CNN) and demonstrate the practicality of ML approaches when large real datasets are difficult to obtain. However, despite these advances, the application of machine learning to molecular communication security remains underexplored.

4) *Authentication Methods:* The unique characteristics of molecular communication and the constraints of developing lightweight security mechanisms limit the direct applicability of traditional authentication schemes to molecular communication systems. Designing authentication methods for biological environments requires significant adaptation to address challenges such as limited computational capacity, memory, energy constraints, and environmental variability. Environmen-

tal factors, such as degradation of molecules in biological fluids or variable diffusion rates, create fluctuating communication channels that complicate consistent authentication. Communication in MC systems is prone to noise, inter-symbol interference, and unintended interactions with other molecules, affecting the reliability of authentication signals. DNA-based and bio-inspired systems enhance origin integrity by mitigating impersonation, sentry, and Sybil attacks.

Recent studies have explored DNA-based molecular security devices that adapt traditional access control mechanisms to molecular environments. Zhang *et al.* introduced a robust two-factor authentication system that combines DNA strand displacement and enzyme cleavage mechanisms [83]. Their approach utilized molecular locks activated by the correct sequence of nicking enzymes, providing security comparable to that of electronic password systems. Bu *et al.* leveraged peptide recognition properties for sensing, encoding, and encryption, demonstrating secure molecular-level information processing and protection [84]. Liu *et al.* developed cryptographic methods using artificial molecules such as p-nitrophenol (PNP) to encode and encrypt data [85]. They incorporated fluorescent molecules to expand detection capabilities and introduced security functions that allowed hidden and encrypted information to be revealed under specific conditions.

Misra *et al.* proposed Bioblock, a blockchain-inspired framework for molecular communication that explores protein-based cryptography [86]. Plasmids are used as carriers of genetic signatures to create blocks that serve as decentralized records. Although Bioblock improves security and eliminates the need for centralized controllers, its consensus mechanism increases latency and energy consumption, creating a trade-off between performance and robustness.

5) *Authentication for Hybrid Networks:* Although bio-nano networks can use MC protocols within their environments, secure communication with macro-scale and EM devices is necessary for widespread adoption. However, interfaces between these paradigms can become potential attack surfaces. It is therefore essential that these interfaces are secured to prevent malicious actors for compromising the hybrid system or either of its components. Since bio-nano devices have limited computational resources compared with modern macro-scale and EM devices, security mechanisms for these interfaces must account for these constraints. Rana *et al.* proposed an ECC-based framework for secure communication between nano-devices, nano routers, and macro devices [41]. The system incorporated EM and MC modes, maintaining a lightweight yet secure approach. Zafar *et al.* introduced an artificial neural network (ANN)-based technique to profile normal and abnormal behaviors at nano-device interface points [45]. The particle swarm optimization algorithm improved accuracy while maintaining low computational costs.

C. Availability

The availability of molecular communication channels is essential for continuous and reliable operation, particularly in critical applications such as early disease detection, food safety, and environmental monitoring. Ensuring robust communication requires addressing environmental variability, biological interference, molecular degradation, and resource con-

straints. Molecular communication can be disrupted not only by malicious entities along the propagation path but also by environmental factors, as MC is highly sensitive to variations in the medium that can significantly impair signal transmission. Resilient availability protocols counteract wormhole, jamming, and blackhole attacks with adaptive interference detection and quorum-sensing biofilm suppression techniques. Next, an overview of various strategies for achieving availability is provided, categorized by inter-symbol interference and jamming, and biofilm suppression.

1) *Inter-symbol Interference and Jamming:* Inter-symbol interference and jamming share overlapping effects on molecular communication but differ fundamentally in their origins. ISI occurs unintentionally due to overlapping molecular signals, while jamming is a deliberate attack using external interference. However, both can degrade signal quality and communication reliability. In diffusion and flow-based molecular communication systems, signals can be disrupted by the random release of additional molecules, which exacerbates the inherent Brownian noise and reduces the effective communication range. Environmental dynamics can further act as natural jammers; for example, biological regulation mechanisms such as glucose control in the bloodstream may unintentionally interfere with molecular signaling.

Liu *et al.* explored mitigation strategies for ISI and jamming attacks [87]. Although ISI can be managed with error correction methods, jamming requires additional measures, such as encoding schemes, to obscure molecular signals. Shahbaz *et al.* proposed a jamming-resistant encoding scheme based on hopped repetition codes [49]. The scheme effectively countered memory-less and adaptive jammers by dynamically altering the pre-shared transmission pattern, ensuring secure and robust communication. Molecular communication channels inherently exhibit memory due to diffusion, molecular interactions, and absorption effects, giving rise to significant ISI as molecules from previous transmissions persist and interfere with subsequent ones. This channel memory increases decoding errors, reduces data rates, and complicates mutual information analysis, highlighting the need for specialized modulation, coding, and detection techniques to mitigate memory-induced performance degradation in molecular and nano-scale systems [37], [68].

In walkway-based propagation using molecular motors, bio-nanomachines can use a network of microtubules to transport large molecules along predetermine pathways. Specifically, it utilizes kinesin and dynein motor proteins with chemical energy from adenosine phosphate to move molecules. This allows molecules to be transported against concentration or flow gradients. Chahibi *et al.* proposed an end-to-end solution to model artificial molecular motor networks and study cargo movements in neurofilaments [88]. Their findings highlight the role of microtubule jamming in brain diseases and offer insights into the creation of artificial systems to counteract these effects. Mangoud *et al.* proposed a Multiple Input, Multiple Output (MIMO) paradigm using microtubule networks in molecular communication [89].

Borrowing the concept from EM communication, information source and information sinks have access to multiple

nodes where each node in the source is connected to every node in the sink with an individual channel link (e.g. a micro-tubule path). Traditional MIMO EM techniques can be adapted for molecular communication to improve channel availability, especially at long distances. Throughput can be enhanced by breaking the message up and sending it simultaneously across different links. Error rates can be reduced by sending the same message across different links for redundancy, making it easier for the message to be recovered assuming that each link experiences loss differently. Enomoto *et al.* proposed a self organizing microtubule network for nanomachines, allowing for a decentralized structure utilizing the channel properties of walkway-based communication [90].

2) *Biofilm Suppression*: Malicious agents may disrupt molecular communication by forming biofilms that prevent signal propagation. Addressing biofilm formation is critical for maintaining communication efficiency in nano-communication systems. Molecular communication channels can be classified as bounded or unbounded depending on the presence of physical constraints in the propagation medium [91], [92]. In unbounded channels, molecules diffuse freely without encountering obstacles, whereas bounded channels, which are more representative of real environments, are constrained by physical boundaries such as cell membranes or other structures that can cause molecular reflection, absorption, or chemical reactions, thereby altering molecular concentration and spatial distribution [93]–[97].

Martins *et al.* demonstrated how bacteria cooperate to block nutrients from reaching biofilms, effectively starving and dismantling the biofilm structure [98]. Gulec *et al.* leveraged quorum sensing mimickers to disrupt biofilm communication pathways. The state-based chemical reaction model effectively simulated biofilm breakdown [52]. Martins *et al.* used proteomic data to identify proteins critical for biofilm formation [50]. By deploying synthetically engineered bacteria to emit jamming signals, protein production essential for biofilm stability is suppressed. It revealed how the distance and delay of jamming signals influenced biofilm disruption, providing insights for designing effective suppression techniques.

Bernal *et al.* explored two quorum-based strategies to mitigate distributed denial-of-service (DDoS) based cyber-bio-attacks aimed at preventing the construction of bacterial biofilms [51]. In the quorum quenching approach, the system emitted enzymes to destroy attack particles; the quorum amplification approach, by contrast, boosted the concentration of molecules necessary to create biofilms. Quorum quenching was found to generally be more successful in mitigating attacks, achieving similar results for a variety of attack patterns. The results of quorum amplification were found to vary more depending on the specifics of the attack pattern.

IV. GAPS AND PROMISING DIRECTIONS

A. Gaps

Despite the focus on confidentiality [39], [40], [53], [69], practical strategies to secure MC channels remain inadequate. Many models assume simplified point-source transmitters and static interference [56], limiting their applicability to real-world molecular communication systems. A broader range of release models and receiver designs should be explored

to generalize secrecy metrics, e.g., diffusive molecular timing channel secrecy. Furthermore, security scheme evaluations are mainly based on simulations conducted in controlled and bounded environments [58]. These fail to capture the complexities of molecular communication, where variable molecular concentrations, unpredictable movements, and ambient noise significantly impact system security and reliability.

Nano-machines face resource constraints that limit the use of traditional security protocols e.g., AES and RSA encryption [99], [100]. Lightweight alternatives inspired by biological systems, including immune-system modeling and cellular communication pathways, have shown promise [101], [102]. Although, interdisciplinary research on security solutions for MC remains underdeveloped. Ensuring data integrity in MC systems is essential, but increasingly challenging due to noise and interference. Noisy molecular channels distort transmitted data, potentially altering information molecules [103]. For example, reactive oxygen species can oxidize signaling molecules [104], leading to corrupt communication. Existing integrity approaches [105], [106] do not adequately address biological noise and environmental changes, which require the development of advanced error detection and correction techniques.

Due to fundamental differences between the communication media, strategies commonly used to analyze and improve secrecy capacity in EM systems may not be directly applicable to MC systems [36]. Studies exploring cooperative jamming, relay nodes, and adaptive modulation [107] highlight potential strategies, but often require substantial coordination and computational resources, introducing additional overhead that is challenging for resource constrained bio-nanodevices. When addressing the risks of eavesdropping, the effects of a dynamic environment are often understudied [33], [34], [100]. In dense molecular networks, attackers may intercept chemical signals without specialized equipment, highlighting the need to develop robust countermeasures. Real-world complexities, such as fluctuating molecular concentrations and unanticipated noise [37], [69] are often overlooked. Comprehensive security frameworks are needed to protect MC systems against unauthorized access and signal alteration.

Temperature, distance, diffusion coefficient, and biological diversity are key factors that directly affect the performance and security of MC systems. *Temperature* variations alter molecular kinetic energy, impacting diffusion rates, reaction kinetics, and signal stability [108]. Even minor fluctuations can increase noise or introduce vulnerabilities in signal propagation. *Distance and diffusion coefficients* causes signal attenuation and delay over long distances amplify interference and reduce effective communication, increasing the likelihood of eavesdropping or denial-of-service (DoS) attacks [56], [69], [109]. *Biological variability* due to environmental randomness—such as fluid dynamics and cellular barriers—compounds the challenges of designing secure MC systems. Failure to account for biological variability can result in unreliable communication and increased susceptibility to interception or signal interruption [110]. These key factors remain insufficiently studied despite their profound impact on molecular communication.

B. Promising Future Directions

The following section discusses potential avenues for developing robust and accurate security mechanisms tailored to molecular and nanocommunication systems.

1) *Cryptographic Methods*: The unique constraints and capabilities of molecular communication networks necessitate the development of specialized cryptographic methods. These approaches must be lightweight, resource-efficient, and capable of leveraging the inherent properties of molecular signals and nanoscale materials. Secure and efficient communication mechanisms can be achieved by integrating advanced encryption techniques with the distinctive characteristics of nanomaterials and biochemical processes.

Further exploration of biochemical cryptographic techniques, which exploit molecular interactions and natural processes to encode information securely is needed. For example, DNA-based cryptography utilizes the complexity and diversity inherent in DNA sequences to encode and decode data [111]. DNA strands store vast amounts of information compactly, making them particularly effective for systems with strict resource limitations. Unlike conventional digital encryption, which may be computationally infeasible for nano-machines, DNA-based encryption leverages biological properties to provide security with low computational overhead.

Molecular steganography is another promising approach in which information is concealed within organic carriers, such as the chemical signals used by cells to communicate [85]. By embedding data within these biological pathways, the method ensures discretion and reduces the risk of interception. For example, chemical signaling molecules can carry encoded information through established biological channels, concealing messages within naturally occurring communication processes, i.e., hiding messages in plain sight. This approach complements traditional cryptographic techniques by adding a layer of obfuscation. The complexity of protein folding or cellular signaling pathways may further increase the difficulty of predicting or replicating these biological processes [112], [113]. Protein folding patterns, for instance, can serve as cryptographic keys, offering a large space of possible configurations. Such natural occurring complexity potentially increases resistance to brute-force attacks.

2) *Error Correction Protocols*: Ensuring data integrity in MC systems prone to high noise levels and interference is a critical challenge. Addressing this challenge requires error detection and correction protocols tailored to the unique characteristics of MC channels to enable robust and reliable communication. Algorithms such as the Tiny Encryption Algorithm (TEA) [114], provide secure and computationally efficient encryption options for molecular communication. These algorithms rely on simple operations, e.g., addition, XOR, and bit shift, ensuring compatibility with the constraints of molecular systems [115]. Additionally, lightweight stream ciphers, such as Grain [116] and Trivium [117], can encrypt data bit by bit, offering efficient encryption for MC systems with modest transmission rates. Integrating keyed hash functions, such as Hash-based Message Authentication Code (HMAC), with error correction [118] ensures that only recipients with the correct key can verify the authenticity and

integrity of the message. This method helps secure transmitted data against unauthorized modifications while maintaining a low computational complexity.

3) *Adaptive Bio-Inspired Solutions*: The design of adaptive security mechanisms for molecular communication systems using principles inspired by biological systems provides robust protection against unauthorized access and should be further explored. For example, leveraging molecular camouflage, selective receptor activation, and other adaptive biological strategies ensures that only designated recipients can decode communication while increasing the resilience of the system against interception.

Molecular camouflage adapts the biological strategy in which organisms blend into the environment to evade predators or threats. [119]. In the context of MC, this approach involves altering the chemical properties of signal molecules to blend with environmental background noise, making the communication signal indistinguishable from naturally occurring metabolites or environmentally benign chemicals. This strategy reduces the likelihood of signal detection by unauthorized entities. For example, signal molecules can be engineered to mimic naturally occurring compounds within the medium, making the communication signal more difficult to detect while preserving its functionality for authorized recipients.

Selective receptor activation mirrors receptor-ligand interactions in biological systems, where only specific receptors can bind to the corresponding ligands [120], [121]. Applied to molecular communication, messages can be encoded to ensure that only devices or recipients equipped with matching receptors can decode and interpret the signal. This creates a secure communication channel where the intercepted signals remain inaccessible to unauthorized entities.

4) *Decentralized Security Solutions*: Decentralized bio-inspired authentication systems should be designed for bio-nanodevices by leveraging their intrinsic properties and interactions, mimicking biological processes such as quorum sensing, the immune response, and swarm intelligence. These approaches establish trust and authenticate devices without relying on centralized control, ensuring resilience and scalability.

Swarm intelligence, inspired by natural systems such as ant colonies and bird flocks, should be further explored in a nano-network communication context [122]. In swarm intelligence, individual entities follow simple, localized rules, which result in emergent, organized behavior. Bio-nanodevices use similar algorithms to self-organize and manage authentication processes without centralized oversight. Such systems can seamlessly adapt to device additions/removals and continuously adjust authentication processes in response to network changes, improving scalability and resilience while reducing vulnerabilities associated with centralized architectures.

5) *Hybrid Communication Networks*: Hybrid communication networks, which combine electromagnetic and molecular communication, offer a versatile and robust solution to address the inherent limitations of each individual communication modality. By dynamically switching between these modalities based on environmental conditions and security requirements, these systems can improve reliability, adaptability, and security in diverse operational contexts.

The Internet of Bio-Nano Things hybrid networks play a critical role in biomedical applications, such as drug delivery, where nano-machines interact with the human body to release medication at precise locations. Secure biochemical communication between nano-machines ensures that only intended recipients activate, reducing errors and adverse effects. This capability significantly improves the precision and safety of medical interventions, making hybrid networks an important component of IoBNT systems [123]. Sun *et al.* proposes a DNA-based MC system for IoBNT using a track-hopper mechanism that enables precise, directional, and low-delay molecular transport. Analysis and simulations demonstrated improved reliability and reduced network delay compared with diffusion-based approaches [124].

Cheng *et al.* proposed an Age of Information (AoI)-driven routing and packet-forwarding framework for DNA-based IoBNT that integrates Markov decision process (MDP)-based routing, multi-retransmission, and Yin-Yang coding to reduce delay, congestion, and errors, with simulations demonstrating improved reliability and overall network performance [125]. In high-EMI environments, such as industrial zones or disaster areas, hybrid networks can enhance the reliability and security of environmental data collection. Molecular communication enables the transmission of ecological data despite electromagnetic noise, helping preserve data integrity and improve monitoring accuracy [36]. In other words, ensuring consistent and secure data flow, despite challenging operational conditions.

V. CONCLUSION

Advancements in molecular communication have the potential to revolutionize fields such as healthcare, environmental monitoring, and smart technology. However, these cutting-edge systems introduce unique security vulnerabilities, including susceptibility to eavesdropping, data integrity breaches, and malicious interference. Addressing these challenges requires the development of novel security mechanisms tailored to the MC paradigm, including bio-inspired approaches, ML-based anomaly detection, environment-aware adaptive protocols, and resource-efficient security techniques. Therefore, an interdisciplinary approach is essential for developing effective security mechanisms for MC.

Future research should focus on integrating security measures that are compatible with the biological environments in which these systems operate. Leveraging innovative approaches, such as DNA-based cryptographic techniques, multi-layered security frameworks, and biomimetic strategies, offer promising directions. The confidentiality, integrity, and availability of transmitted data should be fundamental design objectives rather than afterthoughts, ensuring that molecular communication systems are robust, reliable, and suitable for real-world applications.

REFERENCES

- [1] I. F. Akyildiz, F. Fekri, R. Sivakumar, C. R. Forest, and B. K. Hammer, "Monaco: fundamentals of molecular nano-communication networks," *IEEE Wireless Communications*, vol. 19, no. 5, pp. 12–18, 2012.
- [2] T. Nakano, M. J. Moore, F. Wei, A. V. Vasilakos, and J. Shuai, "Molecular communication and networking: Opportunities and challenges," *IEEE transactions on nanobioscience*, vol. 11, no. 2, pp. 135–148, 2012.
- [3] L. Felicetti, M. Femminella, G. Reali, and P. Liò, "Applications of molecular communications to medicine: A survey," *Nano Communication Networks*, vol. 7, pp. 27–45, 2016.
- [4] M. Ş. Kuran, H. B. Yilmaz, T. Tugcu, and B. Özerman, "Energy model for communication via diffusion in nanonetworks," *Nano Communication Networks*, vol. 1, no. 2, pp. 86–95, 2010.
- [5] W.-A. Lin, Y.-C. Lee, P.-C. Yeh, and C.-h. Lee, "Signal detection and ISI cancellation for quantity-based amplitude modulation in diffusion-based molecular communications," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 4362–4367.
- [6] G. Aminian, M. Mirmohseni, M. N. Kenari, and F. Fekri, "On the capacity of level and type modulations in molecular communication with ligand receptors," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 1951–1955.
- [7] M. U. Mahfuz, D. Makrakis, and H. Mouftah, "Spatiotemporal distribution and modulation schemes for concentration-encoded medium-to-long range molecular communication," in *Proc. of 25th Biennial Symposium on Communications*. IEEE, 2010, pp. 100–105.
- [8] H. B. Yilmaz and C.-B. Chae, "Simulation study of molecular communication systems with an absorbing receiver: Modulation and ISI mitigation techniques," *Simulation Modelling Practice and Theory*, vol. 49, pp. 136–150, 2014.
- [9] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 58–63, 2010.
- [10] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The internet of bio-nano things," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 32–40, 2015.
- [11] N. Ntetsikas, S. Kyriakoudi, A. Kirmizis, B. D. Unluturk, A. Pitsillides, I. F. Akyildiz, and M. Lestas, "Engineering yeast cells to facilitate information exchange," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2024.
- [12] Z. Sakkaff, A. Freiburger, N. Gupta, M. Pierobon, and C. S. Henry, "Information- and communication-centric approach in cell metabolism for analyzing behavior of microbial communities," *bioRxiv*, pp. 2023–08, 2023.
- [13] 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, 2018.
- [14] N. Farsad, H. B. Yilmaz, A. Eckford, C.-B. Chae, and W. Guo, "A comprehensive survey of recent advancements in molecular communication," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1887–1919, 2016.
- [15] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of nano things: Security issues and applications," in *Proc. of the 2018 2nd international conference on cloud and big data computing*, 2018, pp. 71–77.
- [16] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam, and A. Townsend, "Data integrity: Detecting and responding to ransomware and other destructive events," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST Special Publication (SP) 1800-26, Final, December 2020, 2020.
- [17] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks," in *Proc. of IEEE INFOCOM*, vol. 4. IEEE, 2004, pp. 2404–2413.
- [18] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, M. A. Towfiq, and B. A. Cetiner, "Message integrity protection over wireless channel: Countering signal cancellation via channel randomization," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 106–120, 2017.
- [19] W. Guo, Y. Deng, B. Li, C. Zhao, and A. Nallanathan, "Eavesdropper localization in random walk channels," *IEEE Communications Letters*, vol. 20, no. 9, pp. 1776–1779, 2016.
- [20] L. Chouhan and M.-S. Alouini, "Interfacing of molecular communication system with various communication systems over internet of every nano things," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14 552–14 568, 2023.
- [21] M. Pierobon and I. F. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, pp. 602–611, 2010.
- [22] M. Pierobon, "A systems-theoretic model of a biological circuit for molecular communication in nanonetworks," *Nano Communication Networks*, vol. 5, no. 1-2, pp. 25–34, 2014.
- [23] W. Guo, T. Asyhari, N. Farsad, H. B. Yilmaz, B. Li, A. Eckford, and C.-B. Chae, "Molecular communications: Channel model and physical layer techniques," *IEEE Wireless Communications*, vol. 23, no. 4, pp. 120–127, 2016.
- [24] 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.
- [25] A. Ahmadzadeh, A. Noel, and R. Schober, "Analysis and design of multi-hop diffusion-based molecular communication networks," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 2, pp. 144–157, 2015.
- [26] I. Llatser, I. Pascual, N. Garralda, A. Cabellos-Aparicio, M. Pierobon, E. Alarcón, and J. Solé-Pareta, "Exploring the physical channel of diffusion-based molecular communication by simulation," in *Proc. of IEEE Global Telecommunications Conference-GLOBECOM 2011*. IEEE, 2011, pp. 1–5.
- [27] M. Ş. Kuran, H. B. Yilmaz, I. Demirkol, N. Farsad, and A. Goldsmith, "A survey on modulation techniques in molecular communication via

- diffusion," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 7–28, 2021.
- [28] A. M. Abbas, "Molecular nano communication networks: Architectures, protocols and technologies," in *Proc. of 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)*, 2022, pp. 1–5.
- [29] U. A. K. Chude-Okonkwo, R. Malekian, B. T. Maharaj, and A. V. Vasilakos, "Molecular communication and nanonetwork for targeted drug delivery: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 3046–3096, 2017.
- [30] P. Hofmann, J. A. Cabrera, R. Bassoli, M. Reisslein, and F. H. Fitzek, "Coding in diffusion-based molecular nanonetworks: A comprehensive survey," *IEEE Access*, vol. 11, pp. 16411–16465, 2023.
- [31] J. Andréasson and U. Pischel, "Molecules for security measures: from keypad locks to advanced communication protocols," *Chemical Society Reviews*, vol. 47, no. 7, pp. 2266–2279, 2018.
- [32] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Transactions on NanoBioscience*, vol. 13, no. 3, pp. 198–207, 2014.
- [33] Y. Huang, M. Wen, L. Lin, B. Li, Z. Wei, D. Tang, J. Li, W. Duan, and W. Guo, "Physical-layer counterattack strategies for the internet of bio-nano things with molecular communication," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 82–87, 2023.
- [34] S. Qiu, Z. Wei, Y. Huang, M. Abbaszadeh, J. Charment, B. Li, and W. Guo, "Review of physical layer security in molecular internet of nano-things," *IEEE Transactions on NanoBioscience*, 2023.
- [35] S. Zafar, M. Nazir, T. Bakhshi, H. A. Khattak, S. Khan, M. Bilal, K.-K. R. Choo, K.-S. Kwak, and A. Sabah, "A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things," *IEEE Access*, vol. 9, pp. 93 529–93 566, 2021. [Online]. Available: <https://ieeexplore.ieee.org/document/9467302/>
- [36] 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.
- [37] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, and M. Pierobon, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, pp. 110 687–110 697, 2019.
- [38] 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*, vol. 8, no. 3, pp. 190–201, 2022.
- [39] 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.
- [40] Z. Jia, L. Ma, S. Shen, and X. Jiang, "On secrecy performance in D-MoSK-based 3-D diffusive molecular communication system," *IEEE Transactions on NanoBioscience*, 2023.
- [41] A. Rana, S. Prajapat, P. Kumar, D. Gautam, and C.-M. Chen, "Designing a security framework based on hybrid communication in the internet of nano things," *IEEE Internet of Things Journal*, 2023.
- [42] V. Nellore, S. Xi, and C. Dwyer, "Self-assembled resonance energy transfer keys for secure communication over classical channels," *ACS nano*, vol. 9, no. 12, pp. 11 840–11 848, 2015.
- [43] V. Honary and T. A. Wysocki, "Molecular communication system with non-absorbing receiver," *Nano Communication Networks*, vol. 28, p. 100335, 2021.
- [44] H. Singh, M. Bala, S. S. Bamber, and M. Angurala, "Detection of wormhole attack via bio-inspired ant colony optimization based trust model in WSN assisted IoT network," *Wireless Personal Communications*, pp. 1–22, 2024.
- [45] S. Zafar, M. Nazir, A. Sabah, and A. D. Jurcut, "Securing Bio-Cyber Interface for the Internet of Bio-Nano Things using Particle Swarm Optimization and Artificial Neural Networks based parameter profiling," *Computers in Biology and Medicine*, vol. 136, p. 104707, Sep. 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0010482521005011>
- [46] N. Kumar and R. Ali, "A smart contract-based 6g-enabled authentication scheme for securing internet of nano medical things network," *Ad Hoc Networks*, vol. 163, p. 103606, 2024.
- [47] J. Wang, B. Yin, and M. Peng, "Diffusion based molecular communication: principle, key technologies, and challenges," *China Communications*, vol. 14, no. 2, pp. 1–18, 2017.
- [48] R. Shrestha, H. Guerboukha, Z. Fang, E. Knightly, and D. M. Mittleman, "Jamming a terahertz wireless link," *Nature Communications*, vol. 13, no. 1, p. 3045, 2022.
- [49] S. Shahbaz, M. Mirmohseni, and M. Nasiri-Kenari, "A jamming resistant molecular communication scheme," *IEEE Transactions on Molecular, Biological, and Multi-Scale Communications*, 2024.
- [50] D. P. Martins, K. Leetanaksakul, M. T. Barros, A. Thamchaipenet, W. Donnelly, and S. Balasubramaniam, "Molecular communications pulse-based jamming model for bacterial biofilm suppression," *IEEE transactions on nanobioscience*, vol. 17, no. 4, pp. 533–542, 2018.
- [51] S. L. Bernal, D. P. Martins, and A. H. Celdrán, "Towards the mitigation of distributed denial-of-service cyberbioattacks in bacteria-based biosensing systems," *Digital Signal Processing*, vol. 118, p. 103241, 2021.
- [52] F. Gulec and A. W. Eckford, "A stochastic biofilm disruption model based on quorum sensing mimickers," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2023.
- [53] G. Sharma and A. Singh, "Secrecy loss in diffusive molecular timing channels," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 8, no. 4, pp. 297–304, 2022.
- [54] 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. [Online]. Available: <https://ieeexplore.ieee.org/document/9982432/>
- [55] 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, Apr. 2016. [Online]. Available: <https://ieeexplore.ieee.org/document/7347397/>
- [56] G. Sharma, R. K. Mallik, N. Pandey, and A. Singh, "Effect of interfering transmitter on the secrecy of diffusive molecular timing channels," *IEEE Transactions on Communications*, 2024.
- [57] N. V. Sabu, N. Varshney, and A. K. Gupta, "3-D diffusive molecular communication with two fully-absorbing receivers: Hitting probability and performance analysis," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 6, no. 3, pp. 244–249, 2020.
- [58] G. Sharma and A. Singh, "Secrecy performance of diffusion based molecular timing channels," *IET Communications*, vol. 15, no. 2, pp. 289–304, 2021.
- [59] 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.
- [60] D. I. Piraner, M. H. Abedi, M. J. Duran Gonzalez, A. Chazin-Gray, A. Lin, I. Zhu, P. T. Ravindran, T. Schlichthaerle, B. Huang, T. H. Beachchild *et al.*, "Engineered receptors for soluble cellular communication and disease sensing," *Nature*, vol. 638, no. 8051, pp. 805–813, 2025.
- [61] F. Meng, W. M. Shaw, Y. K. K. Kam, and T. Ellis, "Engineering yeast multicellular behaviors via synthetic adhesion and contact signaling," *Cell*, vol. 188, no. 18, pp. 4936–4949, 2025.
- [62] M. Deichmann, "Developing synthetic yeast-based cell-cell communication tools for immune cell activation and manipulation," Ph.D. dissertation, Technical University of Denmark (DTU), 2024.
- [63] M. Wang, H. Nan, M. Wang, S. Yang, L. Liu, H.-H. Wang, and Z. Nie, "Responsive dna artificial cells for contact and behavior regulation of mammalian cells," *Nature Communications*, vol. 16, no. 1, p. 2410, 2025.
- [64] H. Moghimianavval, C. Newell, P. Parviziyan, M. J. Booth, and A. P. Liu, "Strategies and applications of synthetic cell communication," *Nature Chemical Biology*, vol. 21, no. 9, pp. 1317–1329, 2025.
- [65] Q. Zhang, J. Zheng, Y. Wang, S. Xu, W. Wang, J. Xu, J.-R. Zhang, F. Li, and J.-J. Zhu, "A diffusion-based synthetic cell communication network enabled by a multitasking deoxyribonucleic acid nanomachine," *Journal of the American Chemical Society*, vol. 147, no. 18, pp. 15 806–15 813, 2025.
- [66] M. Rezaei, M. Chappell, and A. Noel, "General molecular communication model in multi-layered spherical channels," in *ICC 2025-IEEE International Conference on Communications*. IEEE, 2025, pp. 6043–6048.
- [67] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [68] M. Pierobon and I. F. Akyildiz, "Capacity of a diffusion-based molecular communication system with channel memory and molecular noise," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 942–954, 2012.
- [69] L. Mucchi, A. Martinelli, S. Caputo, S. Jayousi, and M. Pierobon, "Secrecy capacity of diffusion-based molecular communication systems," in *Proc. of 13th EAI International Conference on Body Area Networks 13*. Springer, 2020, pp. 103–114.
- [70] X. Huang, Y. Fang, A. Noel, and N. Yang, "Channel characterization for 1-D molecular communication with two absorbing receivers," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1150–1154, 2020.
- [71] I. Isik, M. Rezaei, and A. Noel, "Single input multi output model of molecular communication via diffusion with spherical receivers," *IEEE Transactions on Molecular, Biological, and Multi-Scale Communications*, vol. 11, no. 1, pp. 101–106, 2024.
- [72] S. Dhok, L. Chouhan, A. Noel, and P. K. Sharma, "Cooperative molecular communication in drift-induced diffusive cylindrical channel," *IEEE Transactions on Molecular, Biological, and Multi-Scale Communications*, vol. 8, no. 1, pp. 44–55, 2021.
- [73] N. V. Sabu, A. K. Gupta, N. Varshney, and A. Jindal, "Impact of multiple fully-absorbing receivers in molecular communications," in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2022, pp. 562–567.
- [74] E. Işık, İ. Işık, and M. E. Taşluk, "Effect of the viscosity on molecule reception ratio for mobile nano systems," *Türk Doğa ve Fen Dergisi*, vol. 10, no. 1, p. 171–175, 2021. [Online]. Available: <https://tfdik.org/JA38CS54BX>
- [75] Y. Sun, H. K. Tan, and Y. Chen, "A bio-nano systems interconnection hierarchical network model for targeted drug delivery," *IEEE Internet of Things Journal*, 2025.

- [76] T. Lindahl and R. D. Wood, "Quality Control by DNA Repair," *Science*, vol. 286, no. 5446, pp. 1897–1905, 1999. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.286.5446.1897>
- [77] Y. Erlich and D. Zielinski, "DNA fountain enables a robust and efficient storage architecture," *science*, vol. 355, no. 6328, pp. 950–954, 2017.
- [78] X. Zhang and F. Zhou, "An encoding table corresponding to ASCII codes for DNA data storage and a new error correction method HMSA," *IEEE Transactions on NanoBioscience*, 2024.
- [79] D. Jing and A. W. Eckford, "Lightweight Channel Codes for ISI Mitigation in Molecular Communication Between Bionanosensors," *IEEE Sensors Journal*, vol. 23, no. 13, pp. 13 859–13 867, Jul. 2023, conference Name: IEEE Sensors Journal. [Online]. Available: <https://ieeexplore.ieee.org/document/10134568/?arnumber=10134568>
- [80] Y. Tang, F. Ji, Q. Wang, M. Wen, C.-B. Chae, and L.-L. Yang, "Reed-Solomon Coded Probabilistic Constellation Shaping for Molecular Communications," *IEEE Communications Letters*, vol. 28, no. 2, pp. 258–262, Feb. 2024, conference Name: IEEE Communications Letters. [Online]. Available: <https://ieeexplore.ieee.org/document/10356127/?arnumber=10356127>
- [81] S.-J. Kim, P. Singh, and S.-Y. Jung, "A machine learning-based concentration-encoded molecular communication system," *Nano Communication Networks*, vol. 35, p. 100433, 2023.
- [82] D. Scazzoli, F. Vakiliipoor, and M. Magarini, "Molecular communication data augmentation and deep learning based detection," *Nano Communication Networks*, vol. 40, p. 100510, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1878778924000164>
- [83] X. Zhang, Y. Liu, B. Wang, S. Zhou, P. Shi, B. Cao, Y. Zheng, Q. Zhang, and N. Kirilov Kasabov, "Biomolecule-driven two-factor authentication strategy for access control of molecular devices," *ACS nano*, vol. 17, no. 18, pp. 18 178–18 189, 2023.
- [84] Z. Q. Bu, Q. F. Yao, Q. Y. Liu, M. X. Quan, J. Y. Lu, and W. T. Huang, "Peptide-based sensing, logic computing, and information security on the antimonene platform," *ACS Applied Materials & Interfaces*, vol. 14, no. 6, pp. 8311–8321, 2022.
- [85] Q. Y. Liu, Z. Q. Bu, M. X. Quan, Y. Wu, X. Ding, L. Q. Xia, J. Y. Lu, and W. T. Huang, "A molecular paradigm: "plug-and-play" chemical sensing and crypto-steganography based on molecular recognition and selective response," *Biosensors and Bioelectronics*, vol. 209, p. 114260, 2022.
- [86] S. Misra, S. Pal, and A. Mukherjee, "BioBlock: A Blockchain Analogous Mechanism for Integrity in IoT-Based Drug Delivery Systems," *IEEE Systems Journal*, vol. 17, no. 1, pp. 1000–1007, Mar. 2023, conference Name: IEEE Systems Journal. [Online]. Available: <https://ieeexplore.ieee.org/document/9864052/?arnumber=9864052>
- [87] Q. Liu, P. He, K. Yang, and S. Leng, "Inter-symbol interference analysis of synaptic channel in molecular communications," in *Proc. of IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 4424–4429.
- [88] Y. Chahibi, I. F. Akyildiz, and I. Balasingham, "Propagation modeling and analysis of molecular motors in molecular communication," *IEEE transactions on nanobioscience*, vol. 15, no. 8, pp. 917–927, 2016.
- [89] M. A. Mangoud, M. Lestas, and T. Saeed, "Molecular motors mimo communications for nanonetworks applications," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–5.
- [90] A. Enomoto, M. J. Moore, T. Suda, and K. Oiwa, "Design of self-organizing microtubule networks for molecular communication," *Nano Communication Networks*, vol. 2, no. 1, pp. 16–24, 2011, role of Inter-Disciplinary Research in Nanoscale Communication. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1878778911000184>
- [91] N. Garralda, I. Llatser, A. Cabellos-Aparicio, and M. Pierobon, "Simulation-based evaluation of the diffusion-based physical channel in molecular nanonetworks," in *Proc. of IEEE conference on computer communications workshops (INFOCOM WKSHPs)*. IEEE, 2011, pp. 443–448.
- [92] I. Llatser, E. Alarcón, and M. Pierobony, "Diffusion-based channel characterization in molecular nanonetworks," in *Proc. of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs)*. IEEE, 2011, pp. 467–472.
- [93] A. Noel, K. C. Cheung, and R. Schober, "Optimal receiver design for diffusive molecular communication with flow and additive noise," *IEEE transactions on nanobioscience*, vol. 13, no. 3, pp. 350–362, 2014.
- [94] H. B. Yilmaz, A. C. Heren, T. Tugcu, and C.-B. Chae, "Three-dimensional channel characteristics for molecular communications with an absorbing receiver," *IEEE Communications Letters*, vol. 18, no. 6, pp. 929–932, 2014.
- [95] H. Arjmandi, M. Zoofaghari, and A. Noel, "Diffusive molecular communication in a biological spherical environment with partially absorbing boundary," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 6858–6867, 2019.
- [96] T. M. Duong, S.-H. Hyun, and S. Kwon, "Channel modeling and achievable data rate for 1-D molecular communication in bounded environments," *Computer Networks*, vol. 232, p. 109852, 2023.
- [97] M. Zoofaghari and H. Arjmandi, "Diffusive molecular communication in biological cylindrical environment," *IEEE transactions on nanobioscience*, vol. 18, no. 1, pp. 74–83, 2018.
- [98] D. P. Martins, M. T. Barros, and S. Balasubramaniam, "Using competing bacterial communication to disassemble biofilms," in *Proc. of the 3rd ACM International Conference on Nanoscale Computing and Communication*, 2016, pp. 1–6.
- [99] I. F. Akyildiz and J. M. Jornet, "Electromagnetic wireless nanosensor networks," *Nano Communication Networks*, vol. 1, no. 1, pp. 3–19, 2010.
- [100] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Communication Networks*, vol. 3, no. 3, pp. 151–160, 2012. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1878778912000294>
- [101] T. Nakano, S. Ando, N. Takata, M. Kawada, K. Murguruma, K. Sekiguchi, K. Saito, S. Yonemura, M. Eiraku, and Y. Sasai, "Self-formation of optic cups and storable stratified neural retina from human escs," *Cell stem cell*, vol. 10, no. 6, pp. 771–785, 2012.
- [102] B. T. McLelland, B. Lin, A. Mathur, R. B. Aramant, B. B. Thomas, G. Nistor, H. S. Keirstead, and M. J. Seiler, "Transplanted hESC-derived retina organoid sheets differentiate, integrate, and improve visual function in retinal degenerate rats," *Investigative ophthalmology & visual science*, vol. 59, no. 6, pp. 2586–2603, 2018.
- [103] A. Ahmadzadeh, H. Arjmandi, A. Burkovski, and R. Schober, "Reactive receiver modeling for diffusive molecular communication systems with molecule degradation," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–7, ISSN: 1938-1883.
- [104] H. J. Forman, M. Maiorino, and F. Ursini, "Signaling Functions of Reactive Oxygen Species," *Biochemistry*, vol. 49, no. 5, pp. 835–842, Feb. 2010.
- [105] P. K. Bularasa and S. R. Sahoo, "A robust and secure drug delivery with single transmitter and dual symmetrical receivers in an internet of bio-nano things," *IEEE Internet of Things Journal*, 2024.
- [106] M. S. Leeson and M. D. Higgins, "Forward error correction for molecular communications," *Nano Communication Networks*, vol. 3, no. 3, pp. 161–167, 2012.
- [107] G. Chang, L. Lin, and H. Yan, "Adaptive detection and ISI mitigation for mobile molecular communication," *IEEE Transactions on nanobioscience*, vol. 17, no. 1, pp. 21–35, 2017.
- [108] S. Kumari, S. Singh, R. K. Singh, V. Pandey, D. K. Singh, S. P. Singh, and M. Lakshmanan, "Performance investigation of molecular nano communication over channels under dynamic scenarios," *Wireless Personal Communications*, vol. 131, no. 1, pp. 471–488, 2023.
- [109] N. Farsad, N.-R. Kim, A. W. Eckford, and C.-B. Chae, "Channel and noise models for nonlinear molecular communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 12, pp. 2392–2401, 2014.
- [110] D. Aktas, B. E. Ortlek, M. Civas, E. Baradari, A. B. Kilic, F. E. Bilgen, A. S. Okcu, M. Whitfield, O. Cetinkaya, and O. B. Akan, "Odor-based molecular communications: State-of-the-art, vision, challenges, and frontier directions," *IEEE Communications Surveys & Tutorials*, 2024.
- [111] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, 2000.
- [112] H. A. Scheraga, M. Khalili, and A. Liwo, "Protein-folding dynamics: overview of molecular simulation techniques," *Annu. Rev. Phys. Chem.*, vol. 58, no. 1, pp. 57–83, 2007.
- [113] F. Rao and A. Caflisch, "The protein folding network," *Journal of molecular biology*, vol. 342, no. 1, pp. 299–306, 2004.
- [114] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2*. Springer, 1995, pp. 363–366.
- [115] X. Hou, L. Ga, X. Zhang, and J. Ai, "Advances in the application of logic gates in nanozymes," *Analytical and Bioanalytical Chemistry*, vol. 416, no. 27, pp. 5893–5914, 2024.
- [116] M. Hell, T. Johansson, and W. Meier, "Grain: a stream cipher for constrained environments," *International journal of wireless and mobile computing*, vol. 2, no. 1, pp. 86–93, 2007.
- [117] C. De Cannière, "Trivium: A stream cipher construction inspired by block cipher design principles," in *International Conference on Information Security*. Springer, 2006, pp. 171–186.
- [118] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "RFC 4226: HOTP: An HMAC-Based One-Time Password Algorithm," RFC Editor, USA, Tech. Rep., 2005.
- [119] K. Dettner and C. Liepert, "Chemical mimicry and camouflage," *Annual review of entomology*, vol. 39, no. 1, pp. 129–154, 1994.
- [120] G. Bao and S. Suresh, "Cell and molecular mechanics of biological materials," *Nature materials*, vol. 2, no. 11, pp. 715–725, 2003.
- [121] C. O'Connor, E. Brady, Y. Zheng, E. Moore, and K. R. Stevens, "Engineering the multiscale complexity of vascular networks," *Nature Reviews Materials*, vol. 7, no. 9, pp. 702–716, 2022.
- [122] C. Blum and D. Merkle, *Swarm intelligence: introduction and applications*. Springer Science & Business Media, 2008.
- [123] A. Setia, R. K. Sahu, S. Ray, R. Widyowati, W. Ekasari, and S. Saraf, "Advances in hybrid vesicular-based drug delivery systems: improved biocompatibility, targeting, therapeutic efficacy and pharmacokinetics of anticancer drugs," *Current drug metabolism*, vol. 23, no. 9, pp. 757–780, 2022.
- [124] Y. Sun, W. Cheng, Q. Wang, K. Yang, and Y. Chen, "Advancing the Internet of Bio-Nano Things: A novel DNA-based track-hopper system for enhanced efficiency and reliability," *IEEE Internet of Things Journal*, vol. 12, no. 4, pp. 4144–4157, 2024.
- [125] W. Cheng, J. Fu, Q. Wang, K. Yang, Y. Chen, and Y. Sun, "AoI-

OptiIoBNT: Age of Information-Driven DNA-Based Internet of Bio-Nano Things Optimization,” *IEEE Internet of Things Journal*, 2025.



Malcolm I. Anderson (Student Member, IEEE) is a Ph.D. student in computer science at Washington State University Vancouver in Vancouver, Washington, USA. He received his B.S. degree in computer science from Washington State University Vancouver in 2022. His research interests include wireless networks, dynamic spectrum access, trust and consensus algorithms, and federated learning.



Truc T. Duong (Student Member, IEEE) is a Ph.D student in Computer Science at Washington State University Vancouver. He received both his B.S and M.S. in Computer Science from Washington State University Vancouver. His research interests include wireless networks, dynamic spectrum access, non-orthogonal random access (NOMA) networks, and bio-inspired algorithms for multiple access control (MAC) protocols.



Ebuka Philip Oguchi (Member, IEEE) received the B.Eng. degree in electronic and computer engineering from Nnamdi Azikiwe University, Awka, Nigeria, in 2016, the M.S. degree in computer applied technology from Changchun University of Science and Technology, Changchun, China, in 2020, and the Ph.D. degree in computer science from the University of Nebraska–Lincoln, Lincoln, NE, USA, in 2025. He is currently an Assistant Professor with the Department of Computer and Information Sciences, Spelman College, Atlanta, GA, USA. His research

interests include cybersecurity, wireless network security, authentication and message integrity verification, machine learning for security, underground wireless communications, vehicular networks, and molecular and nano-communication systems. Dr. Oguchi has served as a reviewer for several international conferences and IEEE journals in wireless communications and cybersecurity.



Anna Wisniewska (Member, IEEE) received her Ph.D. in Computer Science from City University of New York in 2019. She is an Assistant Professor of Computer Science at Washington State University in Vancouver, WA. She has lectured at University of California, Berkeley, in the cybersecurity Master’s program and at City University of New York, Hunter College, in the department of Computer Science. Her research interests include emerging wireless communication, bio-inspired networks, cybersecurity, privacy, dynamic spectrum access, vehicular networks,

internet of things (IoT), NOMA, ML applications in networking and network security, and molecular and nano-communication. She has authored papers in flagship networking conferences and journals, including IEEE Transactions on Vehicular Technology (TVT), IEEE INFOCOM, and IEEE ICC. She has served as a TPC member and reviewer for numerous IEEE networking conferences and journals. She served as a board member of IEEE ComSoc N2Women organization from 2020 to 2022.



Nirnimesh Ghose (Senior Member, IEEE) received his Ph.D. in the Electrical and Computer Engineering from the University of Arizona, Tucson in 2019. He is an Associate Professor of computing at the University of Nebraska-Lincoln. He received his MS degree in Electrical and Computer Engineering from the Illinois Institute of Technology, Chicago in 2012, and his B.Tech. degree in Electronics and Communication Engineering from the Uttar Pradesh Technical University (now Dr. A.P.J. Abdul Kalam Technical University), Lucknow, India in 2010. His

research focuses on network security and privacy with applications to emerging wireless networks, cyber-physical systems, the Internet of Things, aviation and transportation networks, and the interaction between cybersecurity and social networks. He has authored papers in flagship security conferences and journals like IEEE Security and Privacy, IEEE INFOCOM, USENIX Security, and IEEE Transactions on Mobile Communications. He has served as a web chair for IEEE CNS 2018 and as a reviewer for numerous conferences and journals.