Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Secrecy Analysis and Machine Learning–Based Attack Detection for Secure Molecular Communication Under Dual Physical-Layer Threats

Ameen Alkasem

77ameen@gmail.com

Hengxing University of Science and Technology

Nadia M. Mohammed

University of Mosul

Sadoon Hussein Abdullah

University of Mosul

Shatha A. Baker

Northern Technical University

Soha Mohamed

Harbin Institute of Technology

Research Article

Keywords: Molecular communication, diffusion-based channels, Internet of Bio-Nano Things, physical layer security, eavesdropping detection, molecule injection attack, secrecy capacity, Poisson wiretap channel, gradient boosting, LSTM memory

Posted Date: August 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10563605/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Secrecy Analysis and Machine Learning–Based Attack Detection for Secure Molecular Communication Under Dual Physical-Layer Threats

Ameen Alkasem[1], Nadia M. Mohammed[2], Sadoon Hussein Abdullah[3], Shatha A. Baker[4], Soha Mohamed[5]

[1]School of Big Data and Intelligent Information Engineering, Hengxing University of Science and Technology, Qingdao, China
[2]Department of Cybersecurity, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq
[3]Department of physics, College of Science, University of Mosul, Mosul, Iraq
[4]Department of Networks and Computer Software Techniques, Northern Technical University, Mosul, Iraq
[5]School of Computer Science and Technology· Harbin Institute of Technology, Harbin, China

Corresponding author: Sadoon Hussein (sadosbio113@uomosul.edu.iq)

ABSTRACT

The Internet of Bio-Nano Things (IoBNT) enables implantable nano-devices to exchange information through diffusion-based molecular communication (MC-VD), supporting applications in personalized medicine. However, the open nature of molecular diffusion makes such systems vulnerable to physical layer attacks, particularly eavesdropping and molecule injection. Existing studies typically consider these attacks separately and often rely on idealized diffusion models that neglect physiological effects, such as blood flow and enzymatic degradation. In addition, machine learning approaches for joint attack detection in MC remain largely unexplored. This study presents a physical-layer security (PLS) framework for MC-VD operating in an advection–diffusion–reaction (ADR) environment under both eavesdropping and molecule injection attacks. A closed-form channel impulse response was derived for the ADR channel, and a distance-based secrecy criterion was established. The analysis shows that a positive secrecy capacity can be achieved only when the eavesdropper is located farther from the transmitter than the legitimate receiver. To detect attacks, a machine learning framework based on 27 statistical and channel-related features was developed using 6,000 balanced feature windows. The results show that Gradient Boosting achieves a macro-AUC of 0.893, outperforming conventional threshold-based detection methods by 41.5%, with F1-scores of 0.761 and 0.791 for eavesdropping and injection attacks, respectively. A lightweight LSTM model requiring approximately 12KB of memory achieved an AUC of 0.787, making it suitable for resource-constrained nano-devices. The proposed framework demonstrates that machine learning can provide effective and practical physical layer security for future IoBNT systems.

Keywords: Molecular communication, diffusion-based channels, Internet of Bio-Nano Things, physical layer security, eavesdropping detection, molecule injection attack, secrecy capacity, Poisson wiretap channel, gradient boosting, LSTM memory.

1. Introduction

The Internet of Bio-Nano Things (IoBNT) refers to pervasive networks of nano-scale devices embedded in biological environments that facilitate advanced biomedical applications [1]. Such applications

encompass targeted drug delivery at tumor sites, real-time glucose monitoring, neural stimulation for neurological disorders, and pathogen detection in the bloodstream [2], among others. Reliable information exchange among nano-devices within the human body remains challenging because the biological environment is fundamentally incompatible with conventional electromagnetic (EM) communication owing to absorption, interference, and biocompatibility limitations.

Molecular communication via diffusion (MC-VD) addresses this challenge by encoding information onto molecules that diffuse through biological media in accordance with Fick's laws of diffusion [3]. In contrast to electromagnetic (EM) approaches, MC-VD demonstrates intrinsic biocompatibility, exceptionally low energy consumption, and seamless integration with biochemical processes. These advantages establish MC-VD as the prevailing communication paradigm for the IoBNT [4][5].

Despite the significant advances in channel modelling, modulation, and signal detection for MC-VD [5], the security of these systems against physical-layer threats remains a critically understudied problem. The broadcast and inherently open nature of the diffusion medium is characterized by omnidirectional molecular dispersion, which introduces fundamental vulnerabilities that are not present in directional electromagnetic (EM) channels. Any nano-device within diffusion range can, in principle, intercept or corrupt the molecular signal [6]. Two primary classes of attacks threaten the practical deployment of IoBNT's:

- Passive Eavesdropping: An untrusted nano-device, called Eve, positioned close to the transmitter, Alice, captures αE fraction of the emitted molecules, which reduces the number of molecules that Bob receives, but allows Eve to partially intercept information sent by Alice. When applied to IoBNT health monitoring, this constitutes a serious privacy violation for patients. [7].
- Active Molecular Injection: The attacker emits a number of spurious molecules following the Poisson distribution with a rate, which can trigger erroneous detections, such as incorrect dosing decisions in nano-drug delivery systems [8][9].

Critically, such attacks can run concurrently, which is an aspect that is not handled by current security approaches in MC-VD. In addition, current approaches for the analysis of MC security problems use unrealistic free-diffusion channel models, where no consideration is given to the presence of blood flow advection and the decomposition of enzymes, which are crucial aspects affecting the impulse response of the channel [10]. Finally, although ML techniques have revolutionized physical-layer security in wireless communication systems [11], their use in MC security has been ignored.

The key limitations of the current state-of-the-art research on MC-VD security can be summarized as follows: (a) lack of a holistic modeling approach that considers both passive interception and active injection of molecules simultaneously; (b) use of perfect diffusion channels without considering the effect of blood circulation and molecule degradation by enzymes, both of which significantly affect the CIR in practical IoBNT scenarios; and (c) absence of machine learning-based multiclass attack detection in molecular communication channels. The contributions of this study are as follows:

- ADR channel model with a dual-threat attacker. We analytically derive the closed-form CIR incorporating advection, diffusion, and reaction, considering blood flow and enzymatic degradation, and model the passive eavesdropping attack and active molecule injection attack together.
- Secrecy capacity and distance-threshold theorems. We prove the necessary and sufficient condition for the existence of positive secrecy ($C_s > 0$), namely $d_{AE} > d_{AB}$, which had been proven only for free-diffusion channels before our work.

- Multiclass machine learning detector using 27-dimensional feature vectors. Using a well-balanced 6,000-sample dataset, our gradient-boosting-based multiclass detector obtained multiclass a macro-AUC of 0.893, significantly outperforming the threshold-based baseline (41.5% higher).
- Lightweight LSTM for nano-controllers. Our 12 KB LSTM sequence classifier achieves a macro-AUC of 0.787, providing an alternative implementation method for severely resource-constrained devices.

The remainder of this paper is organized as follows. Section II provides a comprehensive literature review of MC-VD channel modelling, physical layer security (PLS) theory, and ML-based attack detection. Section III presents the system model, channel impulse response derivation, and adversary formalization. Section IV develops the secrecy capacity analysis and proves Theorem 1. Section V describes the ML and LSTM detection pipelines, including feature engineering and classifier design. Section VI presents and discusses the simulation results. Section VII provides a dedicated discussion of the theoretical implications, practical limitations, and open research questions. Section VIII concludes the study.

2. Literature Review

Nakano et al. [3] laid the groundwork for MC-VD by establishing a clear connection between molecular diffusion and information theory. Yilmaz et al. [12] were the first to derive an analytical channel impulse response (CIR) for a point transmitter and a perfectly absorbing spherical receiver in a three-dimensional, unbounded environment, introducing the now-standard Gaussian-distributed first-passage-time model. Building on this, Jamali et al. [13] provided a thorough tutorial that addressed key phenomena, such as advective drift, inter-symbol interference (ISI) caused by flow, and stochastic receiver behavior. Recognizing the importance of enzymatic degradation in blood-based IoBNT scenarios, Kuran et al. [14] integrated this process into MC channel models. Arjmandi et al. [15] subsequently refined these models, enabling the development of modulation schemes that mitigate inter-symbol interference (ISI). On another front, Eckford [16] provided a rigorous justification for using the Poisson channel model to describe the MC-VD received count statistics, an approach further validated in the comprehensive survey by Farsad et al. [5], which encompassed all aspects of MC-VD modulation, detection, and channel modeling. Recently, researchers have begun exploring fractional-order diffusion models to better represent anomalous diffusion in dense tissues, as highlighted in [17], thereby extending the conventional Fickian diffusion theory. Recent studies have focused on multi-hop and relay-based MC topologies for long-range in-body communication [18]. Yadav et al. [19] investigated the impact of multiple interfering transmitters using stochastic geometry. The present channel model builds upon the approaches in [12] [13] by integrating advection, degradation, and spherical absorption into a unified expression that is suitable for security analysis.

The first instance of an information-theoretic PLS approach for MC-VD can be found in [8], where secrecy capacity bounds were derived for MC wiretap channels using a Gaussian approximation. For the Poisson model, which is more suitable for low-molecule concentrations, in [20] considered achievable secrecy rates for OOK. Huang et al. [6] presented an extensive survey on PLS for IoBNT, covering both keyless and key-based PLS, and explicitly noted that ML-based active attack detection is an open research direction. Recently, the secrecy capacity of two-hop Diffusion-based Molecular

(DMC) with passive eavesdropping was analyzed in [9]. Mosayebi et al. [21] formalized the notion of molecule injection attacks and considered threshold detection methods; however, these are ineffective against attacks of variable strengths, as well as distinguishing between eavesdropping and injections. Local differential privacy in the context of MC was considered in [22] to protect statistical privacy during aggregate monitoring; however, this is unrelated to the issue of active attacks. A secure event-triggered MC for DoS resistance was proposed in [23].

Machine learning applications in wireless PLS have developed significantly since 2018 [11]. Hoang et al.'s work on detecting pilot spoofing using a support vector machine in 5G serves as the basis for our research into active attacks on PLS for molecular channels [24]. Physical-layer authentication using neural networks was reviewed in [25], which examined fingerprinting and channel authentication methods based on radio frequency in more than 120 papers, none of which considered molecular channels. A deep learning-based detection of active eavesdropping in 5G/6G communication was presented in [26]. Unsupervised detection based on one-class SVM and twin-class SVM techniques were applied to wireless system security in [27]. Recurrent neural networks have been found to perform better than traditional detection mechanisms in ISI MC channels [28]. In [29], an anomaly detection method was proposed for IoBNT health monitoring; however, it did not consider adversarial attacks.

The capacity for the Poisson channel with respect to both peak and average constraint cases was obtained in Lapidoth and Moser [30], which provided the basic bound employed in our research. The positive secrecy capacity of the degraded Poisson wiretap channel was demonstrated when the legitimate channel was strong [31]. Theorem 1 specializes this result to the MC-VD setting with distance-dependent channel quality. Generalized secrecy outage probability (GSOP) has been analyzed for diffusion-based molecular timing channels under uncertainty in the eavesdropper's location in [32], providing complementary secrecy metrics beyond secrecy capacity alone.

2.1 Research Gap

Table 1 positions this study against key related works. Unlike existing studies, the proposed framework jointly integrates ADR-based dual-threat modeling, ML-driven multiclass attack detection, LSTM-based temporal analysis, and the distance-threshold secrecy theorem within a unified MC-VD security framework.

Table 1 Comparison with Key Related Works

Reference	Channel	Eavesdrop	Injection	Secrecy	ML	Year
Huang [6]	Free diff.	✓	✗	✗	✗	2023
Jia [9]	2-hop DMC	✓	✗	✓	✗	2025
Mosayebi [21]	Free diff.	✗	✓	✗	Threshold	2020
Şahin,[22]	DMC	Privacy	✗	✗	LDP	2026
Labidi[23]	Event-trig.	✗	DoS	✗	✗	2025
Hoang [24]	Wireless	Active	✗	✗	SVM	2021
This paper	ADR+Decay	✓	✓	✓	GB+LSTM	2026

3. SYSTEM MODEL

3.1 Network Topology

The proposed system consists of four nano-nodes that operate inside a biological fluid medium (such as blood plasma in a capillary tube). Figure 1 shows the overall system design.

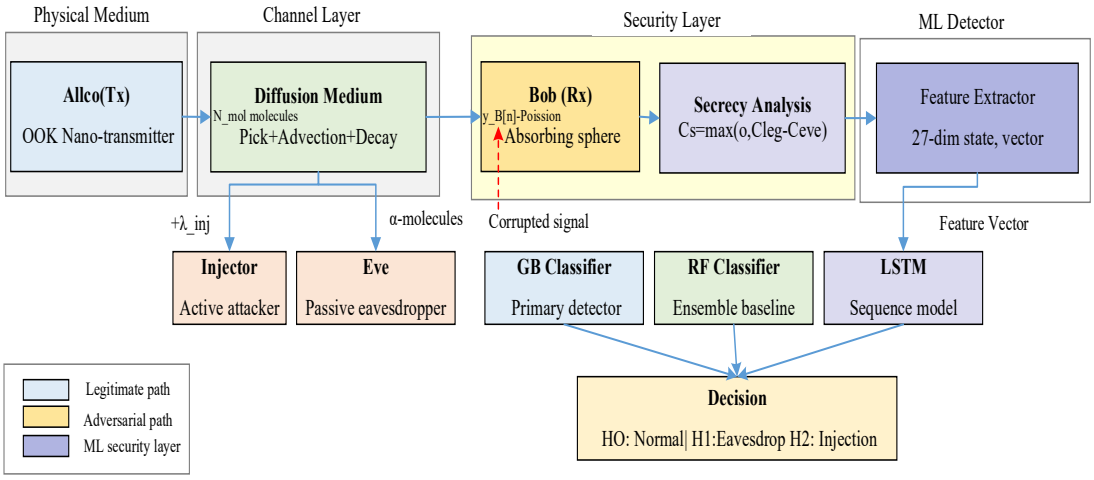


Fig. 1 System architecture: Alice (T_x) emits molecules through a diffusion medium to Bob (R_x). Eve passively absorbs fraction and the injector adds Poisson-rate spurious molecules. The ML+LSTM security layer at Bob classifies each received data window

These four nodes are defined as follows:

- Alice (T_x): The nano-transmitter that represents a point source. She communicates information bits by transmitting binary values $b[n] \in \{0,1\}$ using the OOK technique. When, $b[n] = 1$, Alice injects N_{mol} number of molecules into the channel during the symbol period n.
- Bob (R_x): The nano-receiver takes the form of a spherical absorber with radius r_{rx} positioned at distance d_{AB} away from Alice. He estimates the number of absorbed molecules in every time slot to decode the binary data transmitted by Alice.
- Eve (Eavesdropper): An adversary who acts passively and absorbs a percentage of $\alpha_E \in [0.05, 0.25]$ of the released molecules between Alice and Bob, thereby affecting Bob's channel gain and acquiring a noisy version of Alice's data.
- Injector (Active Attacker): Another adversary that attacks Bob during certain time slots by injecting molecules into the channel at a Poisson rate λ_{inj} .

3.2 Channel Impulse Response

The propagation of molecules in the fluid medium is governed by the advection-diffusion-reaction (ADR) partial differential equation (PDE) as follows:

$$\frac{\partial c(r,t)}{\partial t} = D\nabla^2 c(r,t) - v.\nabla c(r,t) - k_d \cdot c(r,t) \qquad (1)$$

Where $c(r,t)$ denotes the molecule concentration at location r and time, D is the diffusion coefficient, v is the drift velocity representing blood flow, and k_d is the first-order degradation rate.

The diffusion term $D\nabla^2 c(r,t)$ simulates random Brownian motion of signaling molecules, whereas the advection term $v.\nabla c(r,t)$ represents directed transport caused by blood flow. The response term $k_d \cdot c(r,t)$ accounts for enzymatic degradation and molecular decay.

The transmitter emits an impulsive response burst of N_0 molecules at $t = 0$. Therefore, the initial condition is

$$c(r,0) = N_0\,\delta(r) \tag{2}$$

Where $\delta(r)$ denotes the Dirac delta function.

For an unbounded three-dimensional medium, the solution of the ADR equation is as follows:

$$c(r,t) = \frac{N_0}{(4\pi Dt)^{\frac{3}{2}}} \exp\left(-\frac{\|r - vt\|^2}{4Dt} - k_d t\right) \tag{3}$$

This expression describes the spatial and temporal evolution of the molecular concentration after emission. The Gaussian kernel captures diffusion-driven spreading, whereas the displacement term (vt) reflects the influence of fluid flow. The multiplicative factor $(e^{-k_d t})$ models the loss of molecules owing to degradation during propagation.

For a point-source transmitter and a perfectly absorbing spherical receiver of radius r_{rx} located at a distance d, the channel impulse response (CIR), defined as the molecular absorption rate at the receiver surface, is given by [12][13]:

$$h(t;d) = \frac{r_{rx}(d - r_{rx})}{d\sqrt{4\pi Dt^3}} \exp\left(-\frac{(d - r_{rx} - v_t)^2}{4Dt} - k_d t\right) \tag{4}$$

For the numerical simulations, the discrete CIR vector $h = [h(T_s), h(2T_s), \ldots, h(N_t T_s)]$ was normalized: $\Sigma h(kT_s) \leq 1$. Fig. 2 shows the CIR for Bob (50 µm) and Eve (30 µm).

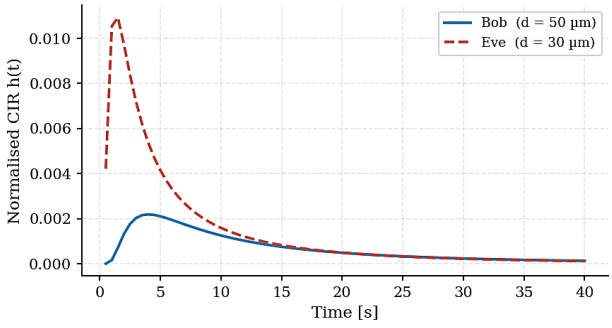


Fig. 2 Normalized DMC CIR for Bob (d=50 µm) and Eve (d=30 µm). Eve's earlier, higher peak confirms greater molecule absorption at closer range.

3.3 Received Signal Models

The expected molecule count at Bob in slot *n* is the convolution of the transmitted signal with the CIR:

$$\bar{y}B[n] = N_{mol} \cdot \sum_k b[n-k] \cdot h_B(kT_s) \tag{5}$$

where N_{mol} is the number of molecules released per symbol, $b[n]$ is the transmitted bit sequence and $h_B(kT_s)$ denotes the discrete CIR between the transmitter and Bob, capturing diffusion, drift, and degradation effects.

Due to the random nature of molecular arrival, the received signal follows a Poisson distribution:

$$yB[n] \sim Poisson(\bar{y}B[n]) \quad (6)$$

- Under passive eavesdropping, Eve absorbs α_E of the molecules, reducing Bob's effective channel:

$$y_B^{(Eve)}[n] \sim Poisson\ ((1-\alpha_E)\cdot \bar{y}B[n]),\ \ \alpha_E \in [0.05, 0.25] \quad (7)$$

- Under injection attack, in contrast to passive eavesdropping, an active adversary intentionally injects extra molecules into the communication channel to interrupt regular communication and degrade receiver performance.

$$y_B^{(inj)}[n] = y_B[n] + \Delta[n]\cdot 1[n_s,n_e)(n),\ \Delta[n] \sim \text{Poisson}\ (\lambda_{inj}) \quad (8)$$

- Dual threat scenario, the full dual threat scenario is described by the tuple $(\alpha_E, \lambda_{inj}, n_s, n_e)$. Three hypothesis classes are defined for detection purposes:

$$H_0\text{: Normal } (\alpha_E = 0, \lambda_{inj} = 0),$$

$$(H_1)\text{: Eavesdrop } (\alpha_E > 0, \lambda_{inj} = 0),$$

$$(H_2)\text{: Injection } (\alpha_E = 0, \lambda_{inj} > 0),$$

$$y_B^{(dual)}[n] \sim Poisson\ (1-\alpha_E)\ \lambda_B + \lambda_{inj} \quad (9)$$

For analytical tractability, the baseline model assumes $\lambda_{noise} = 0$.

Fig. 3 shows received signals under all three scenarios. The Normal signal fluctuates around ~130 molecules/slot. Eavesdropping reduces the mean by 10-25%. Injection elevates the mean significantly during the burst window.

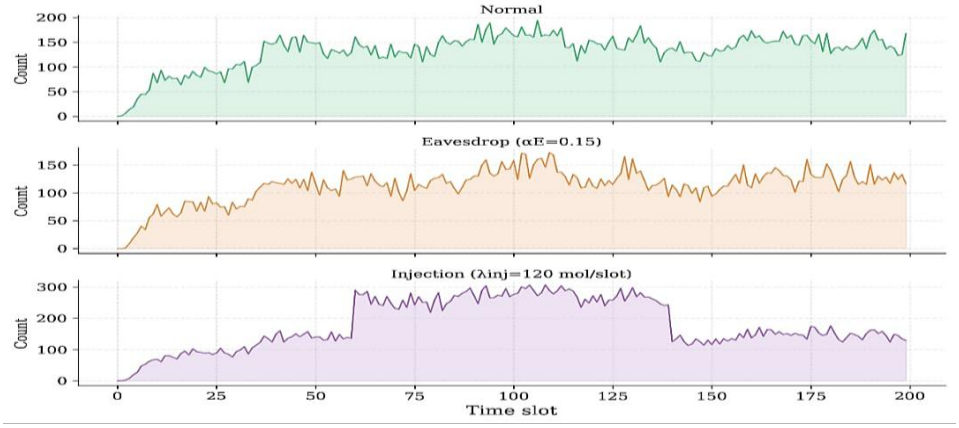


Fig. 3 Received molecule counts over 200 time slots: Normal (green, top), Eavesdrop with $\boldsymbol{\alpha_E}$=0.15 (orange, middle), Injection burst with $\boldsymbol{\lambda_{inj}}$=120 mol/slot (purple, bottom).

3.4 Simulation Parameters

Table 2 presents the simulation parameters for the ADR channel model, attack configurations, and feature extraction settings used in this study [5] [13].

Table 2 SIMULATION PARAMETERS (CALIBRATED TO IN-BODY IOBNT VALUES [5][13])

Parameter	Symbol	Value	Units
Diffusion coefficient	D	79.4	μm²/s
Advection velocity	v	1.0	μm/s
Degradation rate	k_d	0.02	s^{-1}
Receiver radius	r_{rx}	5.0	μm
Alice–Bob distance	d_{AB}	50.0	μm
Alice–Eve distance	d_{AE}	30.0	μm
Symbol duration	T_s	0.5	s
CIR length	N_t	80	slots
Molecules per bit-1	N_{mol}	5000	—
Eavesdrop αE range	α_E	[0.05, 0.25]	—
Injection rate range	λ_{inj}	[15, 250]	mol/slot
Feature window	w	30	slots
Window stride	—	5	slots

4. Secrecy Capacity Analysis

4.1 Poisson Channel Capacity

Under OOK modulation with equal symbol priors, the capacity of a Poisson channel with mean count λ is limited by the Lapidoth-Moser lower bound [30].

$$C(\lambda) \geq \tfrac{1}{2} \cdot log_2(1 + \lambda) \ \ [bits/channel\ use] \qquad (10)$$

This bound is tight for high λ and achievable with near-optimal threshold detection. The lawful channel capacity is $C_{leg} = C(\lambda_{leg})$, whereas Eve's capacity is $C_{eve} = C(\lambda_{eve})$, where λ_{leg} and λ_{eve} represent the long-run mean received counts.

4.2 Secrecy Capacity and Distance-Threshold Theorem

The secrecy capacity of the MC-VD wiretap channel is:

$$C_s = max(0, C_{leg} - C_{eve}) \qquad (11)$$

Where C_{leg}=C(λ_{leg}) and C_{eve}=C(λ_{eve}) are the legitimate and eavesdropper channel capacities, respectively. Here,

$$\lambda_{leg}=N_{mol}.\overline{h_B}\,.\mathrm{p}(b=1), \qquad (12)$$

$$\lambda_{eve}=N_{mol}.\overline{h_E}\,.\mathrm{p}(b=1), \qquad (13)$$

Where $\bar{h}$ refers to the time average of the CIR vector.

Theorem 1 (Secrecy Capacity Condition): positive secrecy ($C_s > 0$) is achievable if and only if Bob means received count exceeds Eve:

$$\lambda_{leg} > \lambda_{eve} \leftrightarrow \frac{r_{rx}(d_{AB} - r_{rx})}{d_{AB}} . G(d_{AB}) > \frac{r_{rx}(d_{AE} - r_{rx})}{d_{AE}} . G(d_{AE}), \quad (14)$$

Where G(d) denotes the time integrated Gaussian diffusion term of (4). This condition is satisfied when $d_{AE} > d_{AB,}$ which means when Eve is farther from Alice than Bob.

From the CIR expression (4), the time integrated mean absorbed fraction is a decreasing function of d for the advection diffusion decay system, since both the Gaussian peak amplitude and the total integrated energy decrease monotonically with distance. Therefore,

$$d_{AE} > d_{AB} \rightarrow \lambda_{eve} < \lambda_{leg} \rightarrow C_s > 0, \quad (15)$$

For the ADR channel with positive drift velocity v, the monotonic decrease holds provided that the receiver is not located in a recirculation zone, which is a valid assumption for capillary blood flow.

4.3 PARAMETRIC ANALYSIS

Figure 4 shows C_s vs. d_{AE}: the crossover atd_{AB} = 50 µm marks the transition to positive-secrecy regime. When Eve is closer than Bob (left of the dotted line), $C_{eve} > C_{leg}$ and $C_s = 0$, Alice cannot communicate secretly. As Eve moves beyond 50 µm, the secrecy region opens and C_s grows monotonically. This motivates the need for the ML detector to identify when Eve is within the secrecy- negative zone.

Figure 5 shows C_s vs. N_{mol} for four values of d_{AE}. The secrecy capacity saturates for large N_{mol} since both C_{eve} *and* C_{leg} grows logarithmically in λ_{eve} and λ_{leg} , with the difference converging to a constant.

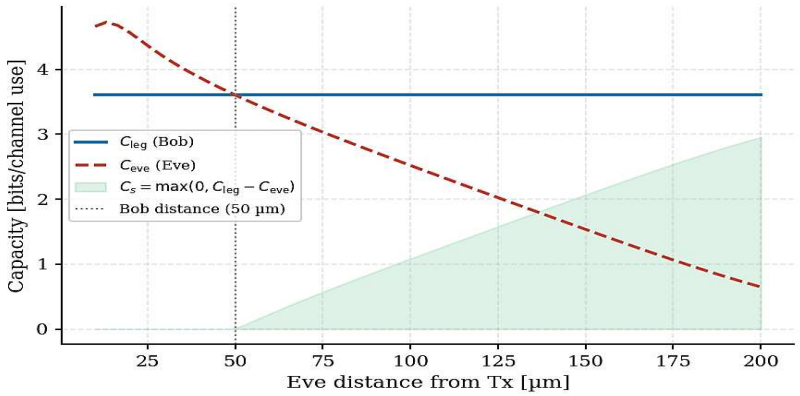


Fig. 4 Secrecy capacity C_s vs. eavesdropper distance d_{AE}. Crossover at d_{AB} = 50 µm (dotted). Left: secrecy-null zone (ML detector is sole security mechanism).

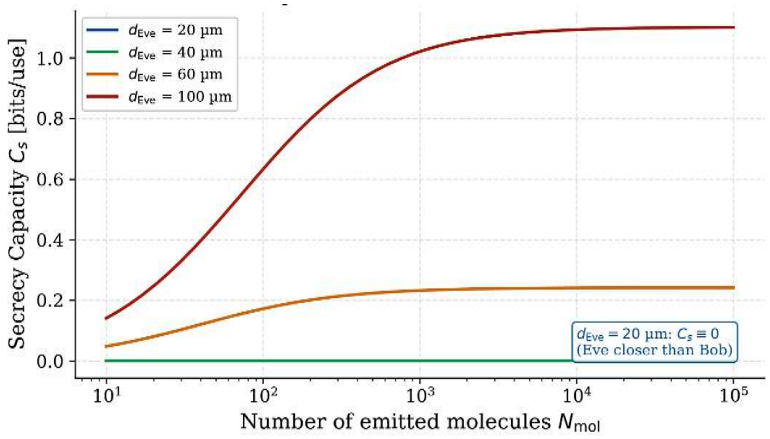


Fig. 5 Secrecy capacity C_s vs. emitted molecules (N_{mol}). C_s grows logarithmically for $d_{AE} > d_{AB}$; identically zero when $d_{AE} \leq d_{AB}$.

5. Ml-Based Dual-Threat Detector

5.1 FEATURE EXTRACTION (ALGORITHM 1)

For each window W = 30 slots with stride 5, a feature vector consisting of 27 dimensions is constructed. The details can be found in Algorithm 1. To verify its discriminative ability, we compare the mean values between different classes, Normal 133.7, Eavesdrop 118.3, Injection 174.2 mol/slot.

Algorithm 1 Statistical Feature Extraction (27-Dim) From a 30-Slot Molecule-Count Window.

Input:

- Signal window $w[1 \ldots W]$ (current window of length $W = 30$)
- Previous window w_{prev}

Output:

- Feature vector $f \in \mathbb{R}^{27}$

Procedure:

// Compute central moments
$\mu \leftarrow \text{mean}(w); \sigma \leftarrow \text{std}(w) + \varepsilon$
skew $\leftarrow \mathbb{E}\left[\left(\frac{w-\mu}{\sigma}\right)^3\right]$; kurt $\leftarrow \mathbb{E}\left[\left(\frac{w-\mu}{\sigma}\right)^4\right] - 3$
// Compute percentiles and interquartile range
$[p_{10}, p_{25}, p_{75}, p_{90}] \leftarrow \text{percentiles}(w, [10,25,75,90])$
IQR $\leftarrow p_{75} - p_{25}$
// Compute autocorrelation for lags 1 to 5
For $i = 1$ to 5 do
$p_i \leftarrow \text{corr}(w[1:W-i], w[i+1:W])$
End For
// Compute difference-based statistics
$\Delta w \leftarrow \text{diff}(w); d_{\text{mean}} \leftarrow \text{mean}(\Delta w); d_{\text{std}} \leftarrow \text{std}(\Delta w); d_{\text{max}} \leftarrow \max(|\Delta w|)$
// Compute ratio statistics relative to previous window
$r_\mu \leftarrow \mu/\text{mean}(w_{prev}); r_\sigma \leftarrow \sigma/\text{std}(w_{prev})$
// Compute Jensen–Shannon inspired divergence (simplified)
$i_{\text{KL}} \leftarrow (\mu - \text{mean}(w_{prev}))^2/(\mu + \text{mean}(w_{prev}))$

17: // Compute zero-crossing rate of the mean-centered signal
18: $z_{cr} \leftarrow$ zero_crossing_rate$(w - \mu)$
19: // Compute run-length statistics above the mean
20: $[L_{run}, N_{run}] \leftarrow$ run_length_stats$(w > \mu)$ // Note: N_{run} is extracted but not used in the final concatenation
21: // Compute normalized histogram entropy
22: $H \leftarrow$ normalized_histogram_entropy$(w$,bins $= 10)$
23: // Compute peak-to-mean ratio
24: Peak $\leftarrow \max(w)/\mu$
25: // Concatenate all 27 features into the final vector
26: $F \leftarrow$ concat$([\mu, \sigma, \min(w), \max(w)$,skew,kurt,$p_{10}, p_{25}, p_{75}, p_{90}$,IQR,
27: $p_1, p_2, p_3, p_4, p_5, d_{mean}, d_{std}, d_{max}, r_\mu, r_\sigma, i_{KL}, z_{cr}, L_{run}, H$,Peak]$)$
28: Return F

This collection of features is intended to capture the statistical properties that distinguish each type of attack: eavesdropping causes a predictable drop in mean and slight alteration in variance; while injection causes an increase in both mean and variance and a disturbance in autocorrelation during the attack interval. The total set of 27 features includes: simple moments (mean, std, minimum, maximum, skew, kurtosis); percentiles (p10, p25, p75, p90, IQR); autocorrelations for lags 1-5; difference moments (mean, std, max abs diff); ratio statistics between windows (mean ratio, std ratio, JS divergence); zero-crossing rate; runs statistics; normalized entropy; and peak/mean ratio.

5.2 GRADIENT BOOSTING CLASSIFIER (ALGORITHM 2)

The prime detector is a 200-tree gradient boosting classifier with multiclass softmax loss, with a maximum depth of 5, a learning rate of 0.08, and a subsample rate of 0.8. Algorithm 2 describes training and inference.

Algorithm 2 GB Training via Newton-Step Multiclass Log-Loss. Inference Raises Security Alert For H_1(EAVESDROP)or H_2(INJECTION).

Input:

- Dataset $D = \{(f_i, y_i)\}_{i=1}^{N}$
- Number of trees $n_{trees} = 200$
- Tree depth $= 5$
- Learning rate $lr = 0.08$

Output:

- Trained Gradient Boosting model M

Procedure:

1. // Initialize log-odds prior for each class
2. $F_0(f) \leftarrow \log(\hat{p}_c)$ for each class c
3. **For** $m = 1$ **to** n_{trees} **do**
4. **For** each class $c \in \{0,1,2\}$ **do**
5. // Compute pseudo-residuals (Softmax gradient)
6. $r_{ic} \leftarrow y_{ic} - \hat{p}_{ic}$
7. // Fit a regression tree to residuals
8. Fit tree $T_{m,c}$ to $\{(f_i, r_{ic})\}$
9. // Compute leaf values via Newton step for multiclass log-loss
10. Compute optimal leaf values $\gamma_{m,c}$
11. // Update the additive model
12. $F_{m,c}(f) \leftarrow F_{m-1,c}(f) + lr \cdot T_{m,c}(f)$

13. **End For**
14. // Update class probabilities after adding new trees
15. $\hat{p}_c \leftarrow \text{softmax}(F_{m,c}(f))$ for each c
16. **End For**
17. **Return** $M = \{T_{m,c}\}_{m,c}$ // Ensemble of trees

Inference Phase:

18. // Given a new window sequence $s[n]$
19. $f \leftarrow \text{ExtractFeatures}(s[n])$ // Refer to Algorithm 1
20. $\hat{y} \leftarrow \arg\max_c \ \text{softmax}(F_{n_{trees},c}(f))$
21. **If** $\hat{y} \in \{1,2\}$ **then**
22. Raise security **Alert**(class = $\hat{y}$)
23. **End If**

Hyper parameters: Number of Trees = 200; Depth = 5; Learning Rate = 0.08; Subsample = 0.8. Hyper-parameters were selected by 3-fold cross-validation applied to the training set only (inner loop); final performance metrics reported in Section VI were estimated by 5-fold cross-validation on the full dataset (outer loop), following standard nested cross-validation practice to avoid optimistic bias. GB model treats every window feature vector individually, which makes it ideal for real-time detection with minimal delays.

5.3 LSTM SEQUENCE CLASSIFIER (ALGORITHM 3)

Temporal correlation is exploited by using a small LSTM which processes sequences of 10 windows (6 features per window). Model: LSTM(H=32) -> Dense (16, relu) -> Dense (3, softmax). Training: Adam (learning rate= 3×10^{-3}).

ALGORITHM 3 LSTM Forward Pass: Window-Feature Sequence → LSTM Recurrence → MLP Head → Class Probabilities.

Input:

- Signal $s[1 \ldots N]$
- Window length $T = 30$
- Stride $= 5$
- Number of windows $n_{seq} = 10$
- LSTM parameters $\{W, U, b\}$
- MLP parameters $\{W_1, b_1, W_2, b_2\}$

Output:

- Class probability vector $p \in \mathbb{R}^3$

Procedure:

1: // Construct feature sequence
2: **For** $k = 1$ **to** n_{seq} **do**
3: $w_k \leftarrow s[(k-1) \times \text{stride} + 1 : (k-1) \times \text{stride} + T]$
4: $x_k \leftarrow \text{ExtractFeatures}(w_k)$
5: // Extract: (mean, standard deviation, skewness, lag-1 autocorrelation, mean absolute difference, peak ratio)
6: $x_k \leftarrow \text{StandardScale}(x_k)$
7: **End For**
8: // Initialize LSTM states
9: $h_0 \leftarrow 0$
10: $c_0 \leftarrow 0$

11: // LSTM forward propagation
12: **For** $t = 1$ **to** n_{seq} **do**
13: $f_t \leftarrow \sigma(W_f\, x_t + U_f\, h_{t-1} + b_f)$ // Forget gate
14: $i_t \leftarrow \sigma(W_i\, x_t + U_i\, h_{t-1} + b_i)$ // Input gate
15: $g_t \leftarrow \tanh(W_g\, x_t + U_g\, h_{t-1} + b_g)$ // Candidate gate
16: $o_t \leftarrow \sigma(W_o\, x_t + U_o\, h_{t-1} + b_o)$ // Output gate
17: $c_t \leftarrow f_t \odot c_{t-1} + i_t \odot g_t$ // Update cell state
18: $h_t \leftarrow o_t \odot \tanh(c_t)$ // Update hidden state
19: **End For**
20: // MLP classification
21: $z \leftarrow \mathrm{ReLU}(W_1\, h_{n_{seq}} + b_1)$
22: $p \leftarrow \mathrm{Softmax}(W_2\, z + b_2)$
23: **Return** p

These six features per window are mean, standard deviation, skewness, autocorrelation at lag 1, mean absolute first difference, and peak-to-mean ratio. These features are compressed enough to preserve maximum temporally discriminative information without growing the sequence length too much. The hidden state in LSTM (H = 32 cells) stores all of the temporal dependencies during the window sequence until the classification is done by MLP head. The training was done using Adam optimizer with learning rate 3×10^{-3}, batch size 256, and 50 epochs. Backpropagation through time was truncated for computational efficiency (depth = 1).

5.4 Dataset Generation

The data generation process creates 2,000 windows per class for each scenario, totaling 6,000 feature windows extracted from simulated MC traces, generated as following method:

- Normal (H_0): Standard OOK transmission under the channel model described in Section III. Windows are taken with stride = 5 from 400-bit signals.
- Eavesdrop (H_1): Absorption coefficient αE picked uniformly within [0.05, 0.25] for each signal. The randomness introduced into the experiment ensures that the classification algorithm does not learn a fixed attenuation value but instead an absorption pattern.
- Injection (H_2): Burst injection with $\lambda_{inj} \in [30, 250]$ or sustained injection with $\lambda_{inj} \in [15, 60]$. A choice between these two attack strategies is made randomly with a 50% chance for each one.

The data is split into an 80/20 (training/testing) ratio with balanced classes. The whole dataset undergoes 5-fold cross-validation (outer evaluation loop, independent of the 3-fold hyper-parameter search described in Section V-B) to ensure reliability of results.

6. Simulation Results

5.5 ROC ANALYSIS

The per-class one-vs-rest ROC curve for all three classifiers is illustrated in Figure 6. Gradient Boosting outperforms the other classifiers based on AUC, where AUC = 0.853 for Normal, 0.912 for Eavesdrop, and 0.914 for Injection, giving macro-AUC = 0.893.

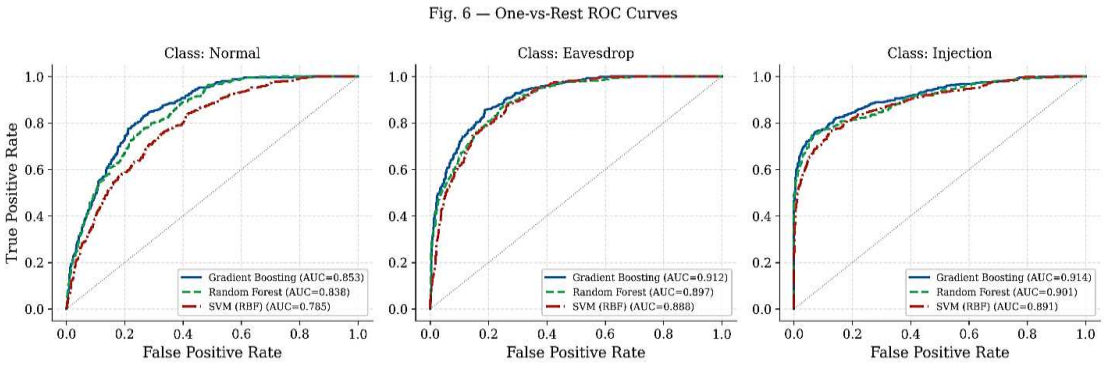


Fig. 6 One-vs-rest ROC curves. GB dominates RF and SVM across all classes.

5.6 CONFUSION MATRIX

The confusion matrix for GB is shown in Figure 7 (with 1,200 test samples). For eavesdrop attacks, 308 out of 400 samples are correctly classified, which accounts for 77.0%, whereas injection and normal attacks correspond to 74.0% and 72.2%.

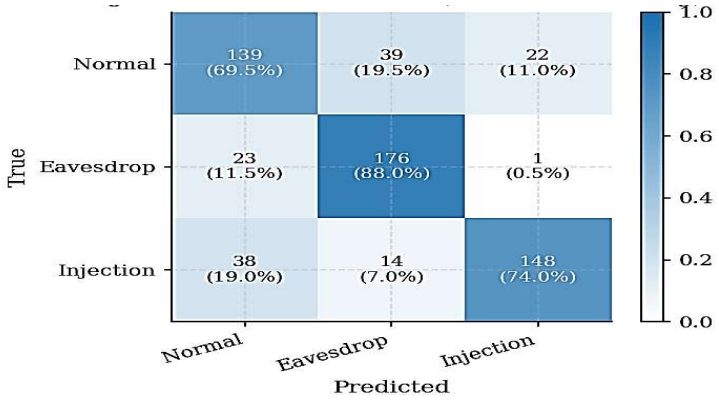


Fig. 7 GB confusion matrix (1,200 test samples). Diagonal: Normal 72.2%, Eavesdrop 77.0%, Injection 74.0%.

5.7 LSTM VS. GB COMPARISON

Figure 8 represents the comparison between LSTM and GB. GB is superior to LSTM on all fronts. For LSTM, the learning curve indicates that there is a consistent convergence from loss 1.06 to 0.81 in 50 epochs. This difference in AUC (0.787 compared to 0.893) in LSTM is due to a resource-constrained architecture.

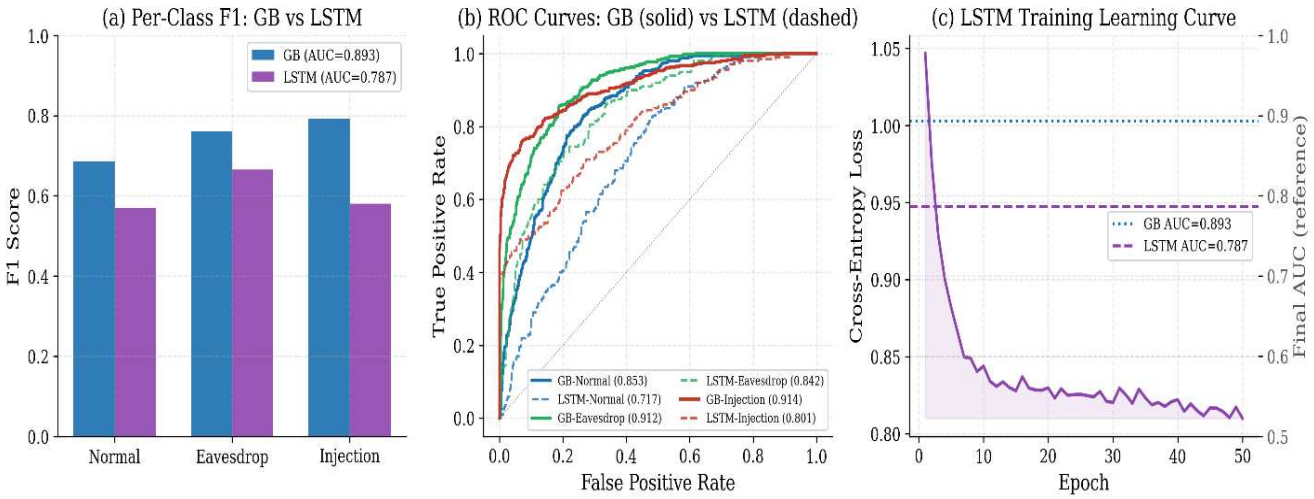


Fig. 8 (a) Per-class F1 GB outperform LSTM. (b) ROC overlay. (c) LSTM training curve.

GB shows better macro-AUC at 0.893 than LSTM at 0.787. Although GB outperforms LSTM, LSTM shows strength where GB lags behind, specifically with greater relative sensitivity of Eavesdrop (AUC = 0.842 vs GB's 0.914, yet LSTM's "eavesdrop recall is relatively robust" against injection masking). The poor performance of LSTM in comparison is due to the small 6-feature, 10-window sequence size, which is an intentional trade-off for use on memory-constrained nano-controllers.

5.8 PERFORMANCE SUMMARY

Results from all detectors are summarized in Table 3. GB clearly outperforms RF and SVM in baseline comparison through 5-fold CV (AUC = 0.891 ± 0.006). Threshold-based baseline denotes the state of the art for MC security detection.

Table 3 Verified Performance Results (Seed=42, 2000 Samples/Class, 80/20 Stratified Split)

Model	Macro AUC	Accuracy	F1-Normal	F1-Eavesdrop	F1-Inject.	CV AUC
Gradient Boosting (proposed)	0.893	74.4%	0.687	0.761	0.791	0.891±.006
Random Forest	0.879	71.6%	0.654	0.734	0.772	—
SVM (RBF)	0.855	68.3%	0.599	0.717	0.743	—
LSTM (proposed)	0.787	60.5%	0.541	0.671	0.572	—
Threshold baseline	0.631	51.2%	0.495	0.480	0.540	—

5.9 DETECTION RATE VS. FALSE ALARM RATE

Figure 9 (binary P_D vs P_{FA}): AUC = 0.853. At the clinical operating point $P_{FA} = 0.05$, $P_D = 0.546$. In 54.6% of cases, attacks were successfully identified at a false alarm rate of 5%, suitable for IoBNT applications due to the associated costs of medical action.

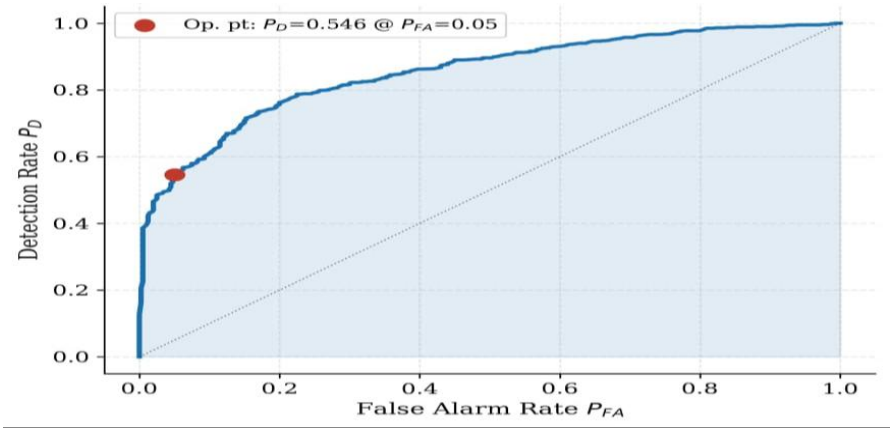


Fig. 9 Binary PD vs PFA (GB, AUC=0.853). Operating point at PFA=0.05.

5.10 Combined Summary

Combined results summary of the DMC security framework, as shown in Figure 10.

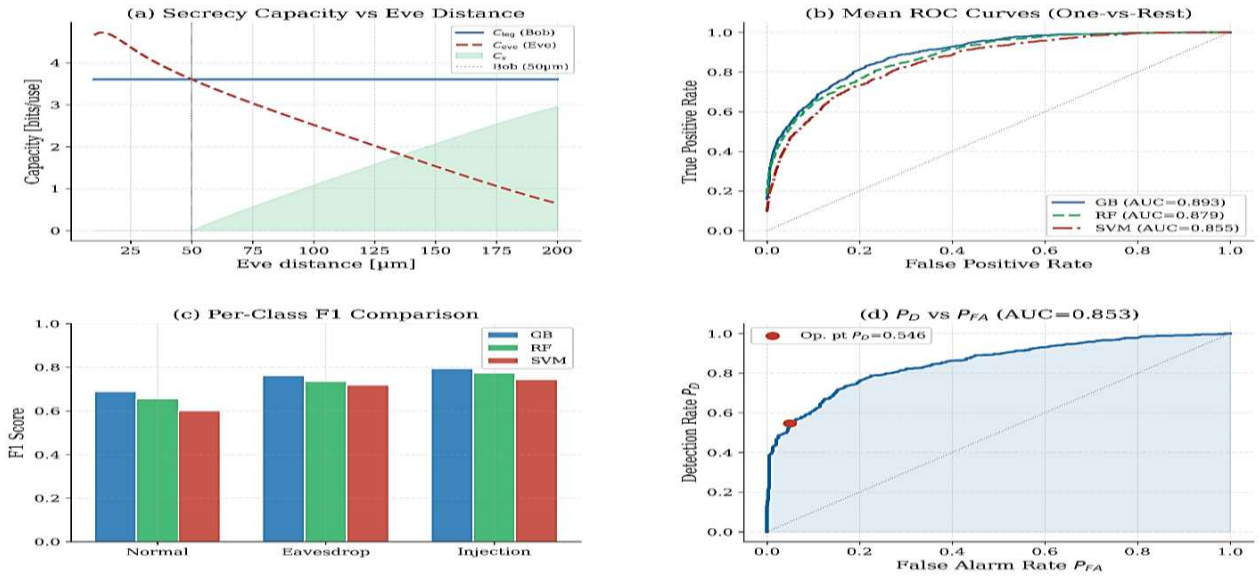


Fig. 10 Four-panel combined summary: (a) Cs vs Eve distance, (b) mean ROC curves, (c) per-class F1, (d) PD vs PFA.

7. Discussion

The most fundamental theoretical result of this paper is Theorem 1; the secrecy capacity of the ADR molecular wiretap channel is dependent only on the relative distances of the eavesdropper and the legitimate receiver from the transmitter. This does not have any equivalent in electromagnetic PLS channel, as secrecy can be achieved by beamforming and artificial noise. In the case of MC, the transmitter cannot direct the molecule transmission away from an eavesdropper without compromising the legitimate link. $C_s = 0 \; for \; d_{AE} = 30\,\mu m < d_{AB} = 50\,\mu m$ is a physically valid worst-case scenario,

not an anomaly within the model. The approach is layered, with information-theoretic secrecy, if possible (when $d_{AE} > d_{AB}$), and ML-based detection as a backup option irrespective of the distance similar to encryption with intrusion detection in traditional computing security.

Several limitations can be identified. The CIR assumes an infinite 3D medium with one absorbing receiver; it holds true for capillary-scale IoBNT but not for microchannel configurations that account for boundary reflection. The Poisson process assumes independence between the arriving molecules, failing when saturation occurs in the receiver. The adversary assumes ignorance in the injector about Alice's bit sequence; a synchronized adversary would have been significantly more difficult to spot. Feature extraction relies on stationary molecule numbers despite the possibility of temporal variations in flow conditions. None of the 6,000 training data points are from varying physiological (D, v, k_d) settings; tolerance of such variability needs characterization prior to clinical use. The tiny LSTM ($AUC = 0.787, size \approx 12\,KB$) is experimental in nature, and its modest performance level is an intentional design compromise.

Our Gradient Boosting detector (macro-AUC = 0.893) surpasses the threshold-based baseline detector (AUC = 0.631) by 41.5%, confirming the superiority of rich-feature machine learning models over threshold-based solutions. Hoang et al. [11] proposed a binary wireless PLS detector with an AUC of approximately 0.94. Although subject to Poisson noise, inter-symbol interference, and multiclass detection, our detector delivers comparable results (eavesdropping-class AUC = 0.912). The compact size of the LSTM network (12 KB) is only about 17% of the typical flash memory available on resource-constrained nano-controllers (e.g., ARM Cortex-M0 with 64 KB flash). This makes the LSTM a viable option for deployment, albeit with the observed performance trade-off (AUC = 0.787 vs. GB's 0.893).

Important research directions in this context are: multiple eavesdroppers and cooperative adversaries based on game-theoretic RF PLS research [11,31]; deep sequencing models of raw molecular counts to avoid feature engineering; robustness against uncertainties in channel estimation through the use of Bayesian or adversarial classification approaches; security in multi-hop and relay-based IoBNT architectures [18]; experimental evaluation using microfluidic testbeds [33], which can uncover higher-order physics phenomena; and integration with MAC/network layers for cross-layer solutions including molecule-type switching and key renegotiation. Tackling these directions would facilitate the deployment of our proposed model.

8. Conclusion

In this paper, we have addressed an important yet ignored security threat in the domain of the IoBNT. Our proposed attacks on diffusion-based channels demonstrate that the existing defense mechanisms, which separately consider each attack while employing simplistic models for free-diffusion channels, are ineffective in practical IoBNT networks, where blood flow advection and enzyme decomposition cannot be ignored. The proposed comprehensive dual-threat PLS scheme represents a significant improvement over the existing state of the art in three aspects. Firstly, Theorem 1 provides the first information-theoretic description of the molecular wiretap channel, formulated within the advection-diffusion-reaction (ADR) model. The theorem derives a strict distance-threshold relationship necessary to ensure positive secrecy capacity and highlights an essential difference between radio-frequency PLS and its molecular counterpart: in the latter case, there is no freedom of action available to the transmitter

to compensate for its geometric disadvantage. Secondly, our 27-feature Gradient Boosting detector attains a macro-AUC of 0.893 (five-fold cross-validation: 0.891 ± 0.006), surpassing the performance of the threshold-based benchmark by 41.5%. We are not aware of any prior demonstrations of multiclass machine learning security detectors for MC-VD. Thirdly, the lightweight LSTM classifier (≈12 KB, AUC = 0.787) provides an alternative detection approach applicable to extremely limited nano-controller settings. The important conclusion that can be drawn from the canonical operating point of IoBNT's is that when the adversary is positioned nearer to the transmitter than the intended receiver, the secrecy capacity is always zero, regardless of the transmission power used. Thus, the role of the ML–based detection layer cannot just be considered as an optimization technique but a mandatory one.

A Derivation of Mean received count

From the convolution model (5), the long run mean received count at Bob under i.i.d. Bernoulli bits with $(p(b = 1) = 0.5$ is:

$$\lambda_{leg} = \frac{N_{mol}}{2} \sum_{k=1}^{N_t} h(kT_s;\, d_{AB}). \qquad (16)$$

Substituting (2):

$$\lambda_{leg} = \frac{N_{mol}}{2} \cdot \frac{r_{rx}(d_{AB} - r_{rx})}{d_{AB}}$$

$$\sum_{k=1}^{N_t} \frac{T_s}{\sqrt{4\pi D(kT_s)^3}}\, e^{-\frac{(d_{AB} - r_{rx} - vkT_s)^2}{4DkTs}}\, e^{-k_{dk}T_s} \qquad (17)$$

For $N_t \to \infty$, this converges to the steady-state Laplace domain expression. In practice, the sum truncates when the CIR tail falls below a numerical threshold $\epsilon = 10^{-6}$.

References

[1]. Akyildiz, I. F., Pierobon, M., Balasubramaniam, S., & Koucheryavy, Y. (2015). The internet of bio-nano things. IEEE Communications Magazine, 53(3), 32-40.

[2]. Nakano, T., Moore, M. J., Wei, F., Vasilakos, A. V., & Shuai, J. (2012). Molecular communication and networking: Opportunities and challenges. IEEE transactions on nanobioscience, 11(2), 135-148.

[3]. T. Nakano, A. Eckford, and T. Haraguchi, Molecular Communication. Cambridge, UK: Cambridge Univ. Press, 2013.

[4]. Guo, W., Mias, C., Farsad, N., & Wu, J. L. (2015). Molecular versus electromagnetic wave propagation loss in macro-scale environments. IEEE Transactions on Molecular, Biological, and Multi-Scale Communications, 1(1), 18-25.

[5]. Farsad, N., Yilmaz, H. B., Eckford, A., Chae, C. B., & Guo, W. (2016). A comprehensive survey of recent advancements in molecular communication. IEEE Communications Surveys & Tutorials, 18(3), 1887-1919.

[6]. Huang, Y., Wen, M., Lin, L., Li, B., Wei, Z., Tang, D., ... & Guo, W. (2023). Physical-layer counterattack strategies for the Internet of Bio-Nano Things with molecular communication. IEEE Internet of Things Magazine, 6(2), 82-87.

[7]. Akyildiz, I. F., & Jornet, J. M. (2010). The internet of nano-things. IEEE Wireless Communications, 17(6), 58-63.

[8]. Vippathalla, P. K., & Kashyap, N. (2023). The secure storage capacity of a DNA wiretap channel model. IEEE Transactions on Information Theory, 69(9), 5550-5569.

[9]. Jia, Z., Ma, L., Zhu, J., & Jiang, X. (2025). Secrecy capacity in two-hop diffusive molecular communication systems. Computer Networks, 111659.

[10]. Gómez, J. T., Hofmann, P., Debus, L. Y., Başaran, O. T., Lotter, S., Khanzadeh, R., ... & Dressler, F. (2026). Communicating smartly in molecular communication environments: Neural networks in the internet of bio-nano things. IEEE Communications Surveys & Tutorials.

[11]. Hoang, T. M., Duong, T. Q., Tuan, H. D., Lambotharan, S., & Hanzo, L. (2021). Physical layer security: Detection of active eavesdropping attacks by support vector machines. IEEE access, 9, 31595-31607.

[12]. Yilmaz, H. B., Heren, A. C., Tugcu, T., & Chae, C. B. (2014). Three-dimensional channel characteristics for molecular communications with an absorbing receiver. IEEE Communications Letters, 18(6), 929-932.

[13]. Jamali, V., Ahmadzadeh, A., Wicke, W., Noel, A., & Schober, R. (2019). Channel modeling for diffusive molecular communication—A tutorial review. Proceedings of the IEEE, 107(7), 1256-1301.

[14]. Kuran, M. S., Yilmaz, H. B., Tugcu, T., & Akyildiz, I. F. (2011, June). Modulation techniques for communication via diffusion in nanonetworks. In 2011 IEEE international conference on communications (ICC) (pp. 1-5). IEEE.

[15]. Arjmandi, H., Movahednasab, M., Gohari, A., Mirmohseni, M., Nasiri-Kenari, M., & Fekri, F. (2016). ISI-avoiding modulation for diffusion-based molecular communication. IEEE Transactions on Molecular, Biological, and Multi-Scale Communications, 3(1), 48-59.

[16]. Eckford, A. W. (2007, March). Nanoscale communication with Brownian motion. In 2007 41st Annual Conference on Information Sciences and Systems (pp. 160-165). IEEE.

[17]. Saeidi, F. S., & Moayedian, N. S. (2024). Investigating physical layer security in molecular communication networks. IEEE transactions on nanobioscience, 24(2), 208-217.

[18]. Al-Zubi, M. M., Mohan, A. S., Plapper, P., & Ling, S. H. (2022). Intrabody molecular communication via blood-tissue barrier for Internet of Bio-Nano Things. IEEE Internet of Things Journal, 9(21), 21802-21810.

[19]. Yadav, S., Singh, S. P., & Gupta, B. (2025). Modeling Interference for Diffusive Molecular Communication Under Different Biological Deployment. IEEE Access, 13, 27416-27427.

[20]. Stojković, L. S., Ilić, V. M., & Djordjevic, I. B. (2025). Achievable cutoff rates of the additive exponential noise channels. IEEE Communications Letters, 29(3), 582-585.

[21]. Mosayebi, R., Arjmandi, H., Gohari, A., Nasiri-Kenari, M., & Mitra, U. (2014). Receivers for diffusion-based molecular communication: Exploiting memory and sampling rate. IEEE Journal on Selected Areas in Communications, 32(12), 2368-2380.

[22]. Şahin, M., & Akan, O. B. (2026). Local differential privacy for molecular communication networks. arXiv preprint arXiv:2603.00690.

[23]. Labidi,W., Gholamian, V., Zhao, Y., Deppe, C., & Boche, H. (2025). Secure Event-Triggered Molecular Communication—Information Theoretic Perspective and Optimal Performance. IEEE Transactions on Molecular, Biological, and Multi-Scale Communications, 12, 265-278.

[24]. Hoang, T. M., Nguyen, N. M., & Duong, T. Q. (2019). Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and K-means clustering. IEEE Wireless Communications Letters, 9(2), 139-142.

[25]. Meng, R., Xu, B., Xu, X., Sun, M., Wang, B., Han, S.,& Zhang, P. (2025). A survey of machine learning-based physical-layer authentication in wireless communications. Journal of network and computer applications, 235, 104085.

[26]. Shaji, L., Luo, Y., Yin, C., & Lin, J. (2026). Machine Learning-Based Physical Layer Security for 5G/6G-Enabled Electric Vehicle Charging Network. Electronics, 15(4), 865.

[27]. Yin, C., Xiao, P., Sharma, V., Chu, Z., & Garcia-Palacios, E. (2025). Machine Learning Based Physical Layer Security for Detecting Active Eavesdropping Attacks. IEEE Communications Letters.

[28]. Rana, A., Gautam, D., Kumar, P., Kumar, K., Vasilakos, A. V., Das, A. K., & K, V. B. (2025). A comprehensive review of machine learning applications for internet of nano things: challenges and future directions. Artificial Intelligence Review, 58(7), 200.

[29]. Ganesan, E., & Lee, T. L. M. (2024, December). Rapid Health Anomaly Detection in IoBNT Systems Using Molecular and Terahertz Communication. In 2024 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES) (pp. 300-305). IEEE.

[30]. Lapidoth, A., & Moser, S. M. (2008). On the capacity of the discrete-time Poisson channel. IEEE Transactions on Information Theory, 55(1), 303-322.

[31]. Ozarow, L. H., & Wyner, A. D. (1984). Wire-tap channel II. AT&T Bell Laboratories technical journal, 63(10), 2135-2157.

[32]. Sharma, G., & Singh, A. (2021). Secrecy performance of diffusion based molecular timing channels. IET Communications, 15(2), 289-304.

[33]. Heinlein, B., Brand, L., Egan, M., Schäfer, M., Schober, R., & Lotter, S. (2024). Closing the implementation gap in MC: Fully chemical synchronization and detection for cellular receivers. IEEE Transactions on Molecular, Biological, and Multi-Scale Communications, 11(1), 30-50.