*mathematics*

MDPI

*Article*

# Machine Learning for Enabling High-Data-Rate Secure Random Communication: SVM as the Optimal Choice over Others

**Areeb Ahmed * and Zoran Bosnić**

University of Ljubljana, Faculty of Computer and Information Science, Večna pot 113, 1000 Ljubljana, Slovenia; zoran.bosnic@fri.uni-lj.si
* Correspondence: areeb.ahmed@fri.uni-lj.si

**Abstract**

Machine learning (ML) has become a key ingredient in revolutionizing the physical layer security of next-generation devices across Industry 4.0, healthcare, and communication networks. Many conventional and unconventional communication architectures now incorporate ML algorithms for performance and security enhancement. In this study, we propose an unconventional, high-data-rate, machine-learning-driven, secure random communication system (HDR-MLRCS). Instead of utilizing traditional static methods to encrypt and decrypt alpha-stable ($\alpha$-stable) noise as a random carrier, we integrated several ML algorithms to convey binary information to the intended receivers covertly. A support vector machine-aided receiver (SVM-R), Naïve Bayes-aided receiver (NB-R), k-Nearest Neighbor-aided receiver (kNN-R), and decision tree-aided receiver (DT-R) were integrated into a single architecture to provide an accelerated data rate with robust security. All intended receivers were pre-trained on a restricted-access dataset (R-$\mathscr{D}$) and exploited a static key—the pulse length—to generate and successfully classify $\alpha$-stable noise samples to extract hidden binary digits. We demonstrated the performance of the proposed HDR-MLRCS by simulating 4-bit and 1000-bit transmissions (including bit error rates and confusion matrices) from the perspectives of the intended receivers and the eavesdropper receiver (E-R). The significance of the HDR-MLRCS lies in its significantly higher data rates compared to previously proposed counterparts using static receivers. At the same time, the SVM-R consistently outperformed all other considered intended receivers. Moreover, the decisive failure of E-R ensures the architecture's resistance to possible interception of communications. The fusion of high data throughput and robustness, enabled by the utilization of ML and $\alpha$-stable noise as a random carrier, highlights the suitability of HDR-MLRCS for future secure communication infrastructures.

**Keywords:** machine learning; SVM; kNN; NB; DT; $\alpha$-stable distributions; covert; random communication system

**MSC:** 68P30

check for updates

Academic Editors: Yufeng Yu, Guoxia Xu and Hu Zhu

Received: 11 October 2025
Revised: 1 November 2025
Accepted: 6 November 2025
Published: 8 November 2025

**Citation:** Ahmed, A.; Bosnić, Z. Machine Learning for Enabling High-Data-Rate Secure Random Communication: SVM as the Optimal Choice over Others. *Mathematics* **2025**, *13*, 3590. https://doi.org/10.3390/math13223590

**Copyright:** © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

Machine learning (ML) has proven its capabilities in transforming conventional methods across all disciplines. ML allows healthcare to analyze complex multimodal datasets to diagnose, predict, and describe diseases through clinical observations [1]. ML has introduced innovative manufacturing systems within Industry 4.0 for real-time fault detection and predictive maintenance [2]. Likewise, the rapid integration of ML with quantum computing has opened a new era of quantum machine learning. It incorporates deep learning

capabilities, quantum computational advantages, and parameterized quantum circuits [3]. Similarly, ML is already playing its role as a catalyst to optimize path optimization, adaptive control, and human–machine collaboration in advanced robotics [4]. Particularly in information and communication technologies, it has critically improved key infrastructure in network optimization, resource allocation, anomaly detection, and security [5]. Taken together, the unimaginable ability of ML to learn complex patterns and provide predictions in highly dynamic environments has established it as a baseline layer for future intelligent systems in the current digital era.

Conventional communication architectures also utilize ML in prominent sub-areas such as resource allocation, error correction, channel estimation, and signal processing [6]. Reliable and renowned ML algorithms such as decision trees (DTs), Naïve Bayes (NB), k-Nearest Neighbors (kNN), support vector machines (SVMs), and neural networks have enhanced the detection capabilities of conventional multi-input multi-output systems [7]. With this development, we have seen an enormous increase in efficiency and a decrease in computational complexity in current conventional communication architectures [8]. Due to this fact, ML-assisted communication systems can now operate under dynamic channel conditions by improving error resilience and assisting resource scheduling [9]. Additionally, error correction and decoding with the help of ML have opened new pathways in wireless communications [10]. The contribution of ML in 5G architectures has provided opportunities for better designs of 6G communication systems.

Research gap: However, with the ever-increasing demand for higher data rates and enhanced security, current conventional communication architectures now possess a limited capacity, after reaching certain thresholds, to integrate ML for further advancements [11]. This limitation motivates exploration of unconventional communication architectures that can better exploit ML for 5G and future 6G systems. The key target is to produce high data throughput for enhanced cybersecurity [12].

Several unconventional techniques have been proposed in the past to enhance the PLS of communication architectures. Spread spectrum (SS) communications was the initiating study that highlighted the need for PLS and explored the benefits of spreading the transmitting sequence bandwidth instead of its original form. The concept remains in place, and many studies continue to utilize it in its optimized form for PLS and performance enhancement [13,14]. Chaotic communication is also notable for its unpredictability, offering secure image encryption through noise signals [15]. It has also demonstrated its coexistence in the 2.4 GHz spectrum in the WiFi and Bluetooth domains [16]. However, SS or chaotic communications suffer from significant code drawbacks, such as sequence predictability, instability of chaotic maps, and lower speed and volume of transmitted information [17].

On the contrary, random communication systems (RCSs) have established themselves as a potential alternative in unconventional secure communications. They utilize $\alpha$-stable noise as a random carrier to covertly convey binary information in a Gaussian channel. On top of that, the RCS has an added layer of security in its architecture. Heavy-tailed distributions with infinite variance negate the applicability of conventional secrecy capacities. We have established the security of a substantial inference gap between the intended receiver with correct parameters and an eavesdropper with no or little information about it. Similarly, side channel attacks are least likely due to the lack of exploitable statistical patterns in $\alpha$-stable noise signals. Since $\alpha$-stable noise samples seem camouflaged within a Gaussian environment, RCSs guarantee that both the binary information and the presence of communication remain concealed in real time [18,19]. Cek [20] and Xu et al. [21] built baseline models with symmetric and skewed $\alpha$-stable noise as carriers to encrypt binary information. They utilized static receivers for successful decryption by intended receivers. Some studies have added single and multiple inverse systems within RCS architecture to

produce an extra key for strengthened security or to provide M-ary transmissions. However, this decreased the data rate [22–24]. RCS architecture has also been successfully validated in the Terahertz band, demonstrating its suitability for current 5G and next-generation 6G systems [25]. Although RCSs have demonstrated theoretical and practical feasibility for covert transmission, they are still lag behind conventional systems due to low data rates despite providing enhanced PLS. Therefore, there is a pressing need for unconventional novel designs that can achieve significantly higher data rates than the current architectures. RCSs with higher data rates are the focus area in unconventional communication systems, where the contribution of ML can substantially boost the overall security of future digital devices.

Given the research gap, the main objectives of the study are as follows:

- Check the multi-classifier architecture of RCS.
- Achieve a higher data rate through RCS by incorporating ML-aided receivers.
- Propose a secure unconventional security architecture.
- Establish performance benchmarks for machine-learning-driven RCSs.

The vital contributions of this study are as follows:

- Multi-classifier architecture of RCSs: To the best of our knowledge, no previous study has conducted a unified comparison of multiple classifiers in $\alpha$-stable random communication systems. Therefore, we have exploited the integration of support vector machines (SVM), Naïve Bayes (NB), k-Nearest Neighbors (kNN), and decision trees (DT) into a single unified design to encrypt and decrypt $\alpha$-stable noise signals.
- Higher data rate: We have achieved significantly higher data throughput for all ML classifiers than previously proposed static estimators. SVMs are prominent among them all. They will help narrow the data throughput gap between unconventional RCSs and conventional communication systems.
- Enhanced security against eavesdropping: The proposed unified architecture also ensures that an eavesdropper fails to extract hidden binary information without a restricted-access dataset and the static pulse length key.
- Benchmark for future research: We have provided comparative performance and security analyses of the renowned ML classifiers for possible integration with RCSs. This can be considered a benchmark for future RCS architecture incorporating ML for developing next-generation secure, covert, and high-rate unconventional communication systems.

The structure of the rest of the paper is as follows: Section 2 provides a brief overview of unconventional secure communications and the contribution of ML in this field. Section 3 provides a detailed explanation of the proposed unified architecture. Section 4 presents the results of Monte Carlo simulations for performance and security evaluation, testing 4-bit and 1000-bit transmissions in terms of bit error rate and confusion matrices. Finally, Section 5 concludes the paper and outlines directions for future research.

## 2. Physical Layer Security via Machine Learning

Given the need to enhance physical layer security (PLS) in conventional communication, studies have integrated ML to achieve three primary purposes: transmitter–receiver authentication, potential intrusion detection, and transmitter–receiver confidentiality formation. Firstly, contributions to the area of authentication have focused on several ML classifiers such as DT, kNN, SVM, and NB. Fang et al. [26] utilized them to explore physical features for precisely estimating channel state information (CSI) and time of arrival, thereby establishing robust authentication architectures. Similarly, a unique combination of machine-learning algorithms, i.e., random forest, and attribute-based authentication presents secure and intelligent IoT applications [27]. Secondly, for intrusion detection

against eavesdropping, attack identification has successfully been optimized in wireless communications by deploying DT, kNN, NB, SVM, and other boosting algorithms [28]. Graph neural networks have upscaled intrusion detection using temporal and multivariate features, jamming, and perimeter detection with the help of curated datasets [29]. Finally, to achieve confidentiality with the help of ML, NB, and SVM, specific approaches have been explored by utilizing partial (where the eavesdropper knows some CSI) and full (where the eavesdropper knows complete CSI) CSI for transmitter antenna selection and channel secrecy [30]. SVM has emerged as a key ML algorithm for effective network detection and ensuring confidentiality under IoT environments [31]. Currently, deep neural networks are the focus points across various disciplines. However, their computational cost and complexity limit their suitability for introductory architectures based on $\alpha$-stable noise carriers. Baseline ML algorithms, especially SVM, NB, kNN, and DT, can be feasibly integrated with conventional architectures. It also prompts the need for unconventional architectures to provide a higher data rate and improved security [32].

Therefore, this paper introduces an unconventional, high-data-rate, machine-learning-driven, secure random communication system (HDR-MLRCS). The design integrates widely used ML algorithms, i.e., SVM, NB, kNN, and DT, in a unified RCS architecture. The proposed architecture is divided into restricted and open-access modes to depict the intended reception scenario and the eavesdropping scenario, respectively. For the restricted-access mode, the HDR-MLRCS performs encryption and decryption of $\alpha$-stable noise to covertly convey binary information from a transmitter to the intended receivers in a additive white Gaussian noise (AWGN) channel. The HDR-MLRCS employs a random noise modulator (RNM), which transmits skewed $\alpha$-stable (Sk$\alpha$S) noise as random carrier signals. The RNM conveys the binary information '0' and '1' by exploiting the inherent skewness of the $\alpha$-stable distribution. The intended receivers, support vector machine-aided receivers (SVM-R), Naïve Bayes-aided receivers (NB-R), k-Nearest Neighborhood-aided receivers (kNN-R), and decision tree-aided receivers (DT-R), are pretrained on a restricted-access dataset (R-$\mathscr{D}$) privately available within the HDR-MLRCS architecture. The R-$\mathscr{D}$ comprises secret values of Sk$\alpha$S noise parameters, mutually selected by RNM and intended receivers, which no eavesdropper can know without prior knowledge. Moreover, the RNM and intended receivers exclusively possess a static secret key—the pulse length—for possible extraction of the binary information from the transmitted signals. Only the intended receivers can perform successful decryption after pretraining through R-$\mathscr{D}$ and utilizing a static secret key. On the contrary, in the open-access mode, the potential eavesdropper-receiver (E-R) attempts decryption using SVM, NB, kNN, and DT, which are pretrained on the open-access dataset (O-$\mathscr{D}$). The O-$\mathscr{D}$ consists of all possible combinations of values of Sk$\alpha$S noise parameters for possible decryption of the transmitted signals. We have shown that the E-R cannot perform any meaningful extraction of the binary information without the knowledge of R-$\mathscr{D}$ and the static secret key. Since the intended receivers could extract binary bits from the fewest number of Sk$\alpha$S noise samples, we achieved very high data rates through HDR-MLRCS compared to previously proposed counterparts. The novel integration of prominent ML algorithms into a single architecture provides enhanced PLS and solves the problem of low data rates encountered by unconventional RCSs. It also shows a comparison of performance among prominent ML algorithms when encrypting and decrypting $\alpha$-stable noise signals. Therefore, the proposed architecture adds value to the category of transmitter–receiver authentication schemes. It incorporates ML to provide boosted PLS and higher data rates. The results collectively demonstrate HDR-MLRCS as a promising unconventional communication paradigm.

## 3. Unified Architecture

We propose a unified architecture for HDR-MLRCS, as shown in Figure 1. It operates in two distinct modes—restricted access and open access—reflecting the perspective of intended receivers and eavesdropper-receivers. Both modes account for a similar AWGN as a channel impairment. The restricted-access mode provides a restricted-access dataset (R-$\mathscr{D}$) and a secret static key to intended receivers for possible extraction of the binary information. The eavesdropper operating in open-access mode must utilize the open-access dataset (O-$\mathscr{D}$) for potential eavesdropping purposes. This section provides a detailed explanation of how both modes and their associated components function.

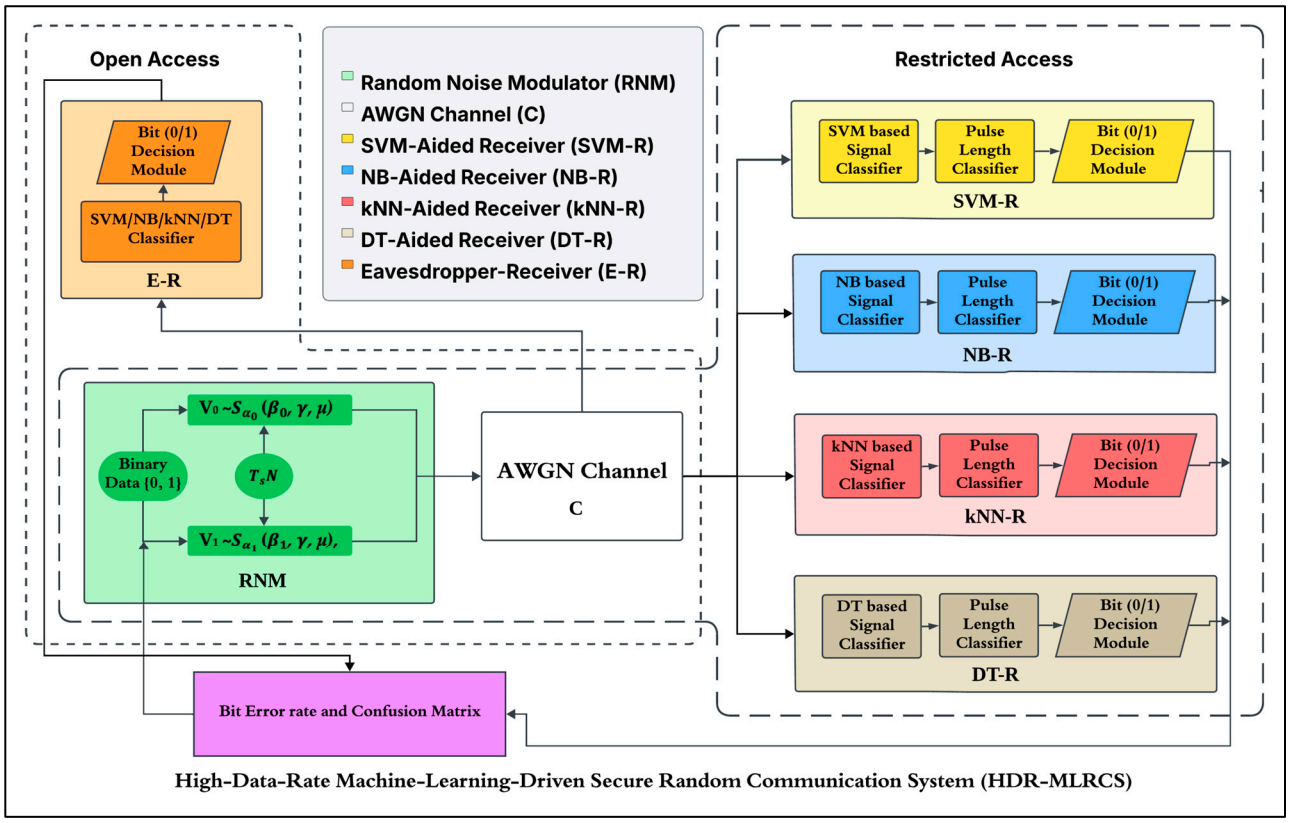



**Figure 1.** Unified architecture of HDR-MLRCS operating in two modes: (1) restricted access with AWGN as channel impairment and (2) open access with AWGN as channel impairment.

### *3.1. Restricted-Access Mode*

The restricted-access mode reflects the process of the proposed transmitter–receiver authentication scheme. We have named the transmitter a random noise modulator (RNM). It conveys binary information by modulating the skewness of $\alpha$-stable noise. We have established four intended receivers, i.e., NB-R, DT-R, kNN-R, and SVM-R, to decrypt the transmitted Sk$\alpha$S noise carriers covertly. AWGN performs channel impairment. Below, we have described all the components required to establish secure communication within restricted-access mode.

#### 3.1.1. Random Noise Modulator (RNM)

The RNM utilizes $\alpha$-stable noise, which is generally famous for characterizing impulsive interference through its powerful statistical model. Secure communications usually utilize it to model impulsive channel conditions by capturing heavy-tailed distributions. $\alpha$-stable noise has been widely tested in various dynamic environments that encounter excessive interference and unpredictable disturbances, such as wireless networks, vehicular

communications, satellite links, and Internet of Things (IoT) applications [33–35]. The $\alpha$-stable distribution relies on four control parameters:

1. The characteristic exponent ($\alpha$) governs impulsiveness and ranges within (0, 2].
2. The skewness parameter ($\beta$) determines distributional asymmetry within $[-1, 1]$.
3. The scale parameter ($\gamma$) controls dispersion over $(0, \infty)$.
4. The location parameter ($\mu$) shifts the distribution along the real axis with $\mu \in (-\infty, \infty)$.

$V \sim S_\alpha\ (\beta, \gamma, \mu)$ denotes the random variable as per the parameters defined above. Some specific distribution cases are more known more prominently, including Gaussian noise, $V_G \sim S_{\alpha=2}\ (\beta = 0, \gamma, \mu)$; Cauchy noise, $V_C \sim S_{\alpha=1}\ (\beta = 0, \gamma, \mu)$; and Lévy noise, $V_L \sim S_{\alpha=0.5}\ (\beta = 1, \gamma, \mu)$. We generated $\alpha$-stable noise through its characteristic function given in [36] as

$$\phi(\theta) = \begin{Bmatrix} \exp\{j\mu\theta - \gamma^\alpha\ |\theta|^\alpha (1 - j\beta\ \mathrm{sgn}(\theta)\tan(\frac{\alpha\pi}{2}))\};\ if\ \alpha \neq 1 \\ \exp\{j\mu\theta - \gamma\ |\theta|(1 + j\beta\frac{2}{\pi}\mathrm{sgn}(\theta)\ln|\theta|)\};\ if\ \alpha = 1 \end{Bmatrix} \quad (1)$$

Other than the defined control parameters $\alpha$, $\beta$, $\gamma$, and $\mu$, Equation (1) contains $j$ as imaginary unit (i.e., $j^2 = -1$) and sgn($\theta$), as sign function (i.e., $\mathrm{sign}(\theta) = 1\ if\ \theta > 0, -1\ if\ \theta < 0,\ 0\ if\ \theta = 0$). The RNM hides the incoming binary data in the skewness parameter of the $\alpha$-stable noise. It follows the principle of noise shift keying. The RNM conveys the incoming binary data '0' and '1' by generating two distinct random carrier signals $V_0 \sim S_{\alpha_0}\ (\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}\ (\beta_1, \gamma, \mu)$, respectively. The skewness parameter satisfies the property of symmetry, i.e., $\beta_1 = -\beta_0$, by shifting the distribution samples towards the left, i.e., $\beta_0 = -1$, or towards right i.e., $\beta_1 = 1$. This deliberate shifting of the distribution enables us to encrypt the binary data '0' and '1' in the samples generated from $V_0 \sim S_{\alpha_0}\ (\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}\ (\beta_1, \gamma, \mu)$, respectively. We have used the term $\Delta\beta \triangleq \beta_1 - (\beta_0)$ to capture the dissimilarity between $\beta_1$ and $-\beta_0$. The quantity of samples required to represent a unit binary digit is called pulse length '$N$' or simply $N$, as $T_U = 1$, which will act as a secret static key for intended receivers. The RNM encodes each bit of binary information into random samples given below as

$$\mathbf{V} = \{v_1, v, \ldots, v_N\} \quad (2)$$

Importantly, no one can recover the encrypted binary data in (2) without absolute knowledge of the $N$. We could have increased the complexity of the encryption by keeping $\alpha_0 \neq \alpha_1$. Still, we kept it identical, i.e., $\alpha_0 = \alpha_1 = \alpha$, to study the effects of skewness on data concealment provided by the HDR-MLRCS. Likewise, we set the location and scale parameters to $\mu = 0$ and $\gamma = 1$. Consequently, the key factors influencing the diversity of the generated $V_0 \sim S_{\alpha_0}\ (\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}\ (\beta_1, \gamma, \mu)$ are $\alpha$, $\Delta\beta$, and N. This makes these parameters an essential part of the restricted-access dataset (R-$\mathscr{D}$) responsible for preserving the covertness of encryption and decryption during transmission and reception, respectively.

Restricted access: To establish covert communications by the proposed HDR-MLRCS, the values of $\alpha$, $\Delta\beta$, $\mu$, $\gamma$, and N were preselected between the RNM and intended receivers. This specific set of values, $\alpha$, $\Delta\beta$, $\mu$, and $\gamma$, acted as dynamic keys. Along with the static key $N$, they provided restricted access to intended receivers by constituting restricted-access keys, given in Table 1 as

**Table 1.** Restricted-access keys.

| **Keys** | **Values** | | |
|---|---|---|---|
| $\alpha$ | 0.6, 0.8, 1.1 | | |
| $N$ | 15, 25, 35 | | |
| $\mu$ | 0 | | |
| $\gamma$ | 1 | | |
| $\Delta\beta$ | 1.6 | 1.8 | 2 |
| Corresponding $\beta_0$ | $-0.8$ | $-0.9$ | $-1$ |
| Corresponding $\beta_1$ | 0.8 | 0.9 | 1 |

The RNM and intended receiver preselect one of the combinations from Table 1 for the decryption of the samples transmitted as $V_0 \sim S_{\alpha_0}(\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}(\beta_1, \gamma, \mu)$, respectively. The choice of the optimal restrictive key values was made by performing exhaustive grid-based search trials covering the key parameter space of the $\alpha$-stable noise-based random communication system. We focused the search on identifying a combination of $\alpha$, $\Delta\beta$, and N that jointly enhanced the performance trends of the $\alpha$-stable noise control factors in HDR-MLRCS. We used the following ranges for the exhaustive search:

- $\alpha$: 0.6–2.0 with increments of 0.1.
- $\Delta\beta$: 0.2–2.0 with increments of 0.25.
- N: 5–500 with increments of 1.

During the exhaustive grid-based search, we set other system parameters, such as $\mu = 0$ and $\gamma = 1$, to maintain comparability across combinations. We ensured accurate noise statistics for each parameter combination while generating $\alpha$-stable noise samples. We have trained and evaluated all intended receivers, i.e., NB-R, DT-R, kNN-R, and SVM-R, under identical conditions. Moreover, we repeated each experiment five times to negate stochastic variation. We selected the parameter combination that yielded the lowest average bit error rate while remaining stable for potential restricted-access keys. We reduced the computational overhead by terminating the exhaustive search when we observed no improvement in the bit error rates over ten consecutive evaluations for the top five parameter sets. The final restricted-access keys listed in Table 1 represent the optimal configurations. We conducted an exhaustive search to achieve optimized BERs for the intended receivers while maintaining covertness. However, real-world deployment or testing for large communication networks under time-varying channels requires offline precomputation, refreshing, and periodically refined keys.

#### 3.1.2. Channel Impairments

Each consecutive transmitted binary information bit, shown in (2), suffers channel impairments in the AWGN channel 'C', which distorts transmitted $V_0 \sim S_{\alpha_0}(\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}(\beta_1, \gamma, \mu)$ via the noise distribution defined as

$$V_G \sim S_{\alpha=2}(\beta = 0, \gamma_G, \mu) \tag{3}$$

Importantly, $V_G$ introduces impairments following sub-characteristics fundamentally present in $\alpha$-stable noise. Since the utilized Sk$\alpha$S noise in the HDR-MLRCS demonstrates an adequate representation of heavy-tailed impulsive phenomena, its noise samples exceed the $V_G$-induced distortions. This is the main reason that the transmitted signals in the HDR-MLRCS remain practically indistinguishable to eavesdroppers, while providing natural resistance to **C**-induced impairments

Similarly, the $\alpha$-stable distribution does not have a second-order moment-generating function, and the first-order moment-generating function also does not exist for $\alpha < 2$.

Therefore, conventional variance-based criteria, such as the 'signal-to-noise ratio,' are not theoretically able to derive the BERs of the HDR-MLRCS. Consequently, mixed signal-to-noise ratio ($MSNR_{dB}$) is used as the standard criterion while measuring $\alpha$-stable random noise of Gaussian environments. It characterizes the ratio between the scale of the transmitted signal $V \sim S_{\alpha}(\beta, \gamma, \mu)$ and of the Gaussian channel noise $V_G \sim S_{\alpha=2}(\beta = 0, \gamma_G, \mu)$, defined below as

$$MSNR_{dB} = 10\log \frac{\gamma}{\gamma_G} \tag{4}$$

We used it to analyze the effects of **C**-induced impairments on $V_0 \sim S_{\alpha_0}(\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}(\beta_1, \gamma, \mu)$. The $MSNR_{dB}$ is measurable in decibels. We used it to examine the HDR-MLRCS while mimicking extreme channel impairments affecting $V_0 \sim S_{\alpha_0}(\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}(\beta_1, \gamma, \mu)$ while traveling in **C**. We have used the scale given below of $\gamma_G$ and the associated $MSNR_{dB}$ in Table 2 to analyze the HDR-MLRCS.

**Table 2. C**-induced impairments.

| Impairment | Values |
|---|---|
| $\gamma_G$ | [0.316, 10] |
| Corresponding $MSNR_{dB}$ | $[-10, 5]$ |
| $\gamma$ | 1 |

3.1.3. Intended Receivers

All intended receivers receive the transmitted **V** in the form of **U**, given below as

$$\mathbf{U} = \mathbf{V} + \mathbf{V_G} \tag{5}$$

The received signal **U** is accessible to both intended receivers and the eavesdropper. However, the intended receivers operate in the restricted-access mode by exploiting the restricted-access dataset. The intended receivers possess dynamic and static keys to perform decryption, hence extracting the hidden binary information concealed in **U**. As shown in Figure 1, we have incorporated SVM-R, NB-R, kNN-R, and DT-R as intended receivers in HDR-MLRCS. All intended receivers are pretrained on a restricted-access dataset (R-$\mathscr{D}$), expressed below as

$$R(\mathscr{D}) = \{(\alpha, \beta, N, MSNR_{dB}, u)\} \tag{6}$$

The values of $\alpha$, $\Delta\beta$, $N$, and $MSNR_{dB}$ come from Tables 1 and 2, respectively. Importantly, 'u' is the resulting Sk$\alpha$S noise sample produced via the specified combination of $\alpha$, $\Delta\beta$, $N$, and $MSNR_{dB}$. Every unique combination in (6) of $\alpha$, $\Delta\beta$, and $N$ from Table 1 and $MSNR_{dB}$ from Table 2 produces a unique 'u', where we took 50 unique realizations of 'u' for a single combination during pretraining of every intended receiver. Following this approach, we trained SVM-R, NB-R, kNN-R, and DT-R on R($\mathscr{D}$) to predict the skewness parameter $\hat{\beta}$. After the successful training phase, the intended receivers learned to predict the output as

$$\hat{\beta} = f(\alpha, N, MSNR_{dB}, u) \tag{7}$$

Regarding the computational environment, we conducted all simulations of $\alpha$-stable noise generation, feature extraction, and associated classifier training/testing in MATLAB R2023a.

**Support vector machine-aided receiver (SVM-R):** The SVM-R operates by approximating the continuous mapping from the feature space to the skewness parameter given in (7), where the regression function is defined as follows:

$$\hat{\beta} = \sum_{i=1}^{m} (\lambda_i - \lambda_i^*) K(x_{new}, x_i) + b \tag{8}$$

where the Lagrange multipliers $\lambda_i$ and $\lambda_i^*$ are obtained during pretraining of SVM-R. $K(.,.)$ is the kernel function. Similarly, $b$ is the bias parameter. Importantly, the mapping of the input features is as follows:

$$x_i = (\alpha,\ \beta,\ \mathrm{N},\ \mathrm{MSNR_{dB}},\ u_i) \tag{9}$$

This mapping of input features into higher-dimensional space is carried out by the $K(.,.)$. We selected the radial basis function $K(.,.)$ after comparing it with linear and polynomial kernels due to superior generalization across $\alpha$-stable noise conditions. We utilized the MATLAB Classification Learner app to optimize the automatic hyperparameters to achieve a box constraint of $C$ = 10, a kernel scale of $\gamma$ = 0.01, and an iteration tolerance based on the 5-fold cross-validation accuracy. Finally, we performed a final evaluation on the test set with the classifier that achieved the highest cross-validation accuracy. The SVM-R predicted the output $\hat{\beta}$ by utilizing kernel-based regression. It modeled the nonlinear relationship between the transmuted $\beta$ ($\beta_0$ or $\beta_1$) and R ($\mathscr{D}$) parameters.

**Naïve Bayes-aided Receiver (NB-R):** The NB-R works on estimating the conditional distribution of $\hat{\beta}$ given in (7). It does so by obtaining a posterior expectation as the regression estimate of transmitted $\beta$ ($\beta_0$ or $\beta_1$) as follows:

$$\hat{\beta} = \mathbb{E}\left[\beta \mid \alpha, N, MSNR_{dB}, u\right] \tag{10}$$

where the posterior density is

$$P(\alpha, N, MSNR_{dB}, u \mid \beta) \propto P(\beta \mid \alpha, N, MSNR_{dB}, u)\, P(\beta) \tag{11}$$

Since the features have conditional independence among themselves, the likelihood further decomposes as follows:

$$P(\alpha, N, MSNR_{dB}, u \mid \beta) = P(\alpha \mid \beta)\, P(N \mid \beta)\, P(MSNR_{dB} \mid \beta)\, P(u \mid \beta) \tag{12}$$

The expression given in (13) helps the NB-R in the approximation of $\hat{\beta}$, which was given in (7). As shown in (11)–(13), we performed it by integrating the contribution of each independent feature distribution. Hence, the regression-based NB-R provides an efficient estimation of $\hat{\beta}$ as given in (7).

**k-Nearest Neighborhood-aided receiver (kNN-R):** The kNN-R computes $\hat{\beta}$, as given in (7), by applying weighted KNN averaging. We calculated the weighted average of the neighboring $\beta_i$ from the received samples of **U**, as given below.

$$\hat{\beta} = \frac{\sum_{i \in N_k} w_i \beta_i}{\sum_{i \in N_k} w_i} \tag{13}$$

where we computed weights between the query point and the i-th neighbor as

$$w_i = \frac{1}{d(x_{new}, x_i) + \epsilon} \quad ;\ \epsilon = 10^{-5} \tag{14}$$

The unique Euclidean distance, $d(x_{new}, x_i)$, in (10) exists between the new sample $x_{new}$ and each training sample $x_i = (\alpha,\ \beta, \mathrm{N}, \mathrm{MSNR}_{dB}, u_i)$. We computed $d(x_{new}, x_i)$ as

$$d(x_{new}, x_i) = \sqrt{(\alpha_{new} - \alpha_i)^2 + (N_{new} - N_i)^2 + (\mathrm{MSNR}_{new} - \mathrm{MSNR}_i)^2 + (u_{new} - u_i)^2} \tag{15}$$

Before training the kNN-R on R($\mathscr{D}$), we standardized all features using z-score normalization, i.e., $\hat{x} = \frac{x_j + \mu_j}{\sigma_j}$. The mean '$\mu_j$' and standard deviation '$\sigma_j$' were calculated using R

($\mathscr{D}$). By doing this, we ensured bias prevention, as every feature contributed proportionally to the Euclidean distance.

**Decision tree-aided receiver (DT-R):** The DT-R works based on the principle of classification and regression trees (CART) algorithm and utilizes binary splitting for the construction of decision trees. The Gini index (*GI*) is the factor that determines the choice to split the attribute variable. The DT-R computes *GI* by utilizing R($\mathscr{D}$) as

$$GI\left[\mathrm{R}(\mathscr{D})\right] = 1 - \sum_{i=1}^{m} p_i^2 \tag{16}$$

Since the purpose of *GI* is to analyze the node's impurity, the value of *GI* equals zero, replicating a pure node. On the contrary, we calculate maximum impurity by judging the maximum classes. The DT-R calculates '*GIS*' as

$$GIS\mathrm{R}(\mathscr{D}) = \frac{j_1}{j} GI\left[\mathrm{R}_1(\mathscr{D})\right] + \frac{j_2}{j} GI\left[\mathrm{R}_2(\mathscr{D})\right] \tag{17}$$

which is the *GI* of the split when splitting R($\mathscr{D}$) into $\mathrm{R}_1(\mathscr{D})$ and $\mathrm{R}_2(\mathscr{D})$. Since 'j' is the size of R($\mathscr{D}$), $\mathrm{j}_1$ and $\mathrm{j}_2$ are the sizes of $\mathrm{R}_1(\mathscr{D})$ and $\mathrm{R}_2(\mathscr{D})$. The DT-R traverses towards the split that attains minimum *GI* for the subsequent subsets. After the successful training phase defined in (12) and (13), the DT-R learns to predict $\hat{\beta}$, as given in (7).

**Static key-based classification:** All intended receivers must perform static key-based classification after estimating $\hat{\beta}$ $N$ times. The multiple predicted $\hat{\beta}$ values, $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_N\}$, hold a single binary information bit, '0' or '1'. It converts every consecutive set, i.e., $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_N\}$, into a single classified binary digit, '$\beta_D$', as per the hard decision given below:

$$\beta_D = \begin{Bmatrix} \beta_0 \,; if \sum_{t=1}^{N} \hat{\beta}_t < 0 \\ \beta_1; if \sum_{t=1}^{N} \hat{\beta}_t \geq 0 \end{Bmatrix} \tag{18}$$

where $\beta_0$ and $\beta_1$ reflect the conversion of $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_N\}$ to the binary information bit '0' or '1', respectively. The procedure repeats itself until all subsequent sets, $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_N\}$, are converted back into binary information. Importantly, the RNM and intended receivers can utilize any one value of $N$ as a static key from restricted-access keys defined in Table 1 for secure communication through the HDR-MLRCS. The smaller $N$ results in a higher data rate, as fewer samples are required to retrieve a unit binary digit.

#### 3.1.4. 4-Bit Transmission

We experimented with a shorter stream of binary information bits, which we refer to as '4-bit transmission'. It gave us clearer insight into and visualization of the encryption and decryption process before we analyzed the HDR-MLRCS on many bits. We demonstrate this proof of concept in Figure 2.

The '4-bit transmission' in Figure 2 shows four incoming binary information bits, "1, 0, 1, 0", and the corresponding encrypted noise signal **V** transmitted from RNM. The received noise signal **U** is accessible to all intended receivers after traversing the AWGN channel. The intended receivers exploit **U** to predict $\hat{\beta}$ and then $\beta_D$ to decrypt the transmitted hidden binary information bits "1, 0, 1, 0". In the 4-bit transmission experiment, we utilized $\alpha = 0.8$ and $N = 15$, where $\Delta\beta = 1.8$, i.e., $\beta_0 = -0.9$ and $\beta_1 = 0.9$, to represent the binary information bits '0' and '1'. The given transmission was tested with $\mathrm{MSNR}_{\mathrm{dB}} = -5$ dB to analyze the decryption capabilities of the intended receivers in severe channel conditions.

We present the initial performance trends of the intended receivers, NB-R, kNN-R, DT-R, and SVM-R, operating in restricted-access mode, through a visual representation of the decryption process in Figure 2. We observed that the prediction capabilities of intended receivers in predicting $\hat{\beta}$ tended to improve gradually for every subsequent set of incoming

values $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_{N=15}\}$ which held a single information bit. This observation applied to all intended receivers regardless of the number of erroneous predicted $\hat{\beta}$ in their first set of $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_{N=15}\}$. Consequently, lesser predicted values of $\hat{\beta}$ were erroneous for every subsequent set of $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_{N=15}\}$ of binary information bits.

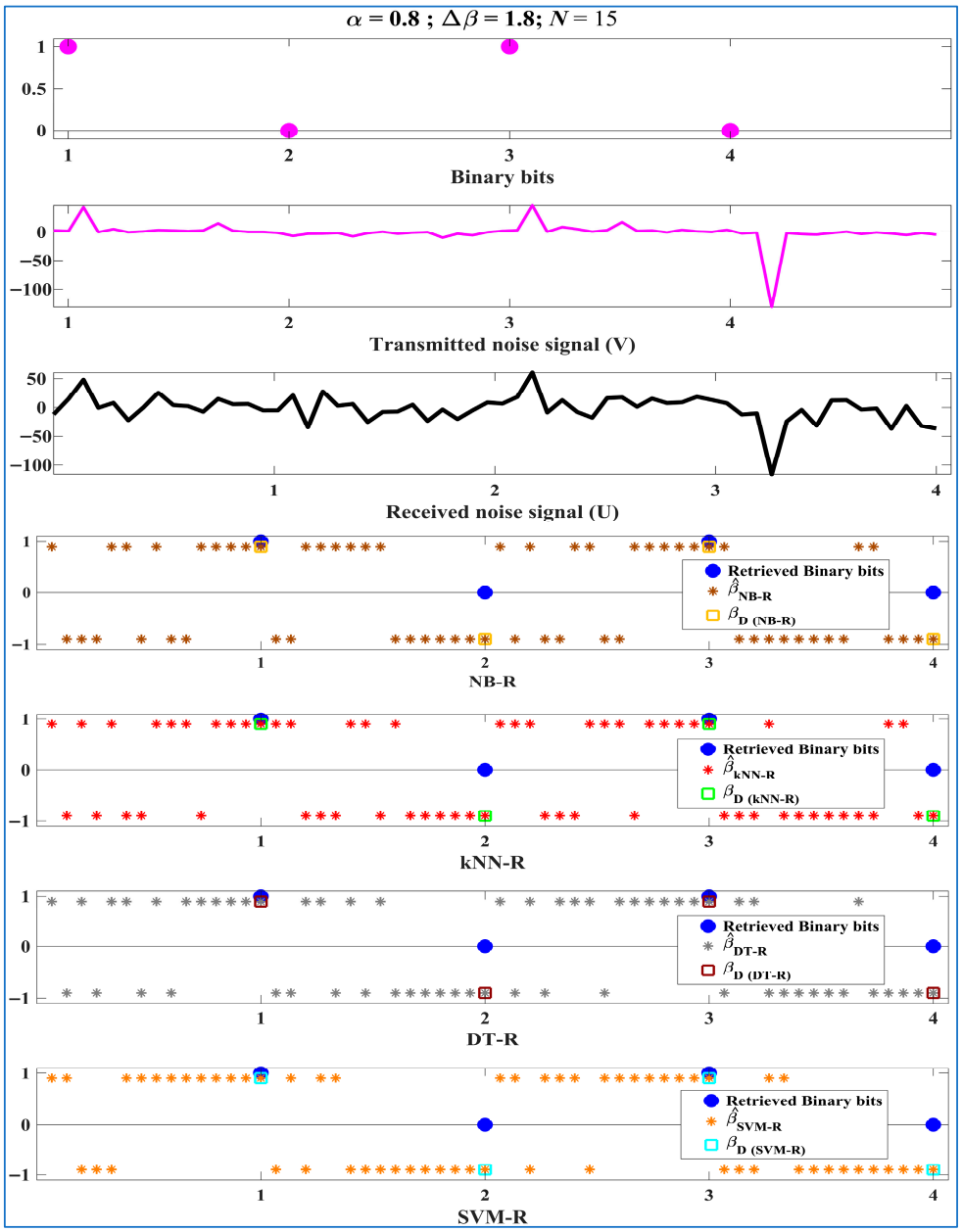



**Figure 2.** Rows 1, 2, and 3: Shorter stream of binary information bits, corresponding transmitted noise signal (**V**) from RNM and received noise signal (**U**). Rows 4, 5, 6, and 7: Predicted skewness parameters $\hat{\beta}$ as outputs, corresponding single classified binary digit $\beta_D$ and retrieved binary bits by intended receivers NB-R, kNN-R, DT-R, and SVM-R, where $\alpha = 0.8$, $\Delta\beta = 1.8$, $N = 15$.

If we consider the first set of predicted values of $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_{N=15}\}$ containing the binary information bit '1' shown in Rows 4–7 in Figure 2, the SVM-R encountered the fewest errors, i.e., three out of fifteen. On the contrary, DT-R, kNN-R, and NB-R encountered five, six, and seven errors, respectively. We also saw similar trends for the later sets of predicted $\{\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_{N=15}\}$ containing "0, 1, 0". This shows the superior decryption capability of SVM-R over the other intended receivers. It is important to note that all intended receivers successfully recovered the transmitted binary information bits "1, 0, 1,

0''. However, analyzing it for a larger number of bits in the later section would further prove the practicality of the proposed HDR-MLRCS.

### *3.2. Open-Access Mode*

Previously, we analyzed the architecture of the proposed transmitter-receiver authentication scheme in restricted-access mode. Therefore, it is also necessary to assess the strength of the HDR-MLRCS against potential eavesdropping. The open-access mode considers the HDR-MLRCS from the perspective of the potential eavesdropper. It also receives the signal traversing through the same AWGN channel. In actual practice, detecting the presence of a communication established by the HDR-MLRCS is impossible. However, we modeled the eavesdropper-receiver (E-R) as a significantly advanced communication interceptor to depict the worst-case scenario for the HDR-MLRCS.

Eavesdropper-Receiver (E-R)

We considered the same signal **U**, which was given in (5) and propagated through the AWGN channel C, to be available to the E-R. As shown in Figure 1, the E-R could utilize any receiver among NB-R, kNN-R, DT-R, and SVM-R to perform possible decryption of the transmitted binary information bits. However, the E-R did not completely possess the restricted-access keys available to intended receivers. Hence, the E-R utilized open-access keys during the training phase.

Open access: Since the actual values of $\alpha$, $\Delta\beta$, and $N$ utilized in restricted-access mode by the RNM and intended receivers were unknown to the E-R, it relied on open-access keys given below in Table 3

**Table 3.** Open-access keys.

| Keys | Values |
|---|---|
| $\alpha$ | $(0, 2]$ |
| $N$ | $[1, \infty]$ |
| $\mu$ | $[-\infty, \infty]$ |
| $\gamma$ | $(0, \infty)$ |
| $\Delta\beta$ | $[0, 2]$ |
| Corresponding $\beta_0$ | $[-1, 0)$ |
| Corresponding $\beta_1$ | $[0, 1]$ |

On top of that, the E-R also possessed the static key $N$. Without the static key, it is theoretically impossible, with a probability of $\frac{1}{\infty}$, to perform any meaningful decryption from **U**. However, we assumed '$N - 1$' as the static key to analyze the HDR-MLRCS under this study's worst-case key leakage scenario. Moreover, we assumed that the E-R had exact knowledge that $\mu = 0$ and $\gamma = 1$ and of the $\alpha$ utilized by the RNM and intended receivers. Otherwise, it would be practically impossible to derive the performance of the E-R. With the given assumption, we analyze the performance of the E-R in the next section.

## 4. Transmission and Analysis

Given the successful 4-bit transmission with one of the selected combinations of the restricted keys ($\alpha = 0.8$, $\Delta\beta = 1.8$, and $N = 15$) at $\text{MSNR}_{\text{dB}} = -5$ dB, we analyzed the HDR-MLRCS for 1000-bit transmission with all possible combinations of the restricted keys. Firstly, we reflected this analysis by computing confusion matrices in this section. Similarly, it was necessary to test the proposed HDR-MLRCS under a versatile range of channel impairments [19–25]. Therefore, later in this section, the BER performances against the versatile range of $\text{MSNR}_{\text{dB}}$ are also derived to reflect the overall performance of the HDR-MLRCS architecture in the AWGN channel. Later, we discuss the most crucial factor,

i.e., the achieved data rate, which is the most significant factor for unconventional random communication systems.

### *4.1. Confusion Matrix Analysis*

We computed 1000-bit confusion matrices for the transmitted and retrieved data according to the HDR-MLRCS architecture, as shown in Figure 1. To derive the performance of intended receivers in the restricted-access mode, we fixed values of μ and γ to '0' and '1', respectively. We derived confusion matrices by keeping two restricted parameters ($\alpha$, $\Delta\beta$, and $N$) fixed while varying the third one to analyze the individual effects on the HDR-MLRCS. In contrast, we derived the confusion matrices for the E-R in the open-access mode while predicting $\hat{\beta}$, as given in (7).

#### 4.1.1. Intended Receivers

In 4-bit transmission, the SVM-R achieved the best performance, while the NB-R was the worst-performing receiver. The SVM-R and NB-R encountered the fewest and the most errors on average, respectively. Building on the above trend, we have focused solely on evaluating the confusion matrices of NB-R and SVM-R in Figures 3 and 4, respectively. The confusion matrices of the kNN-R and DT-R can be assumed to exist somewhere between these two extremes.

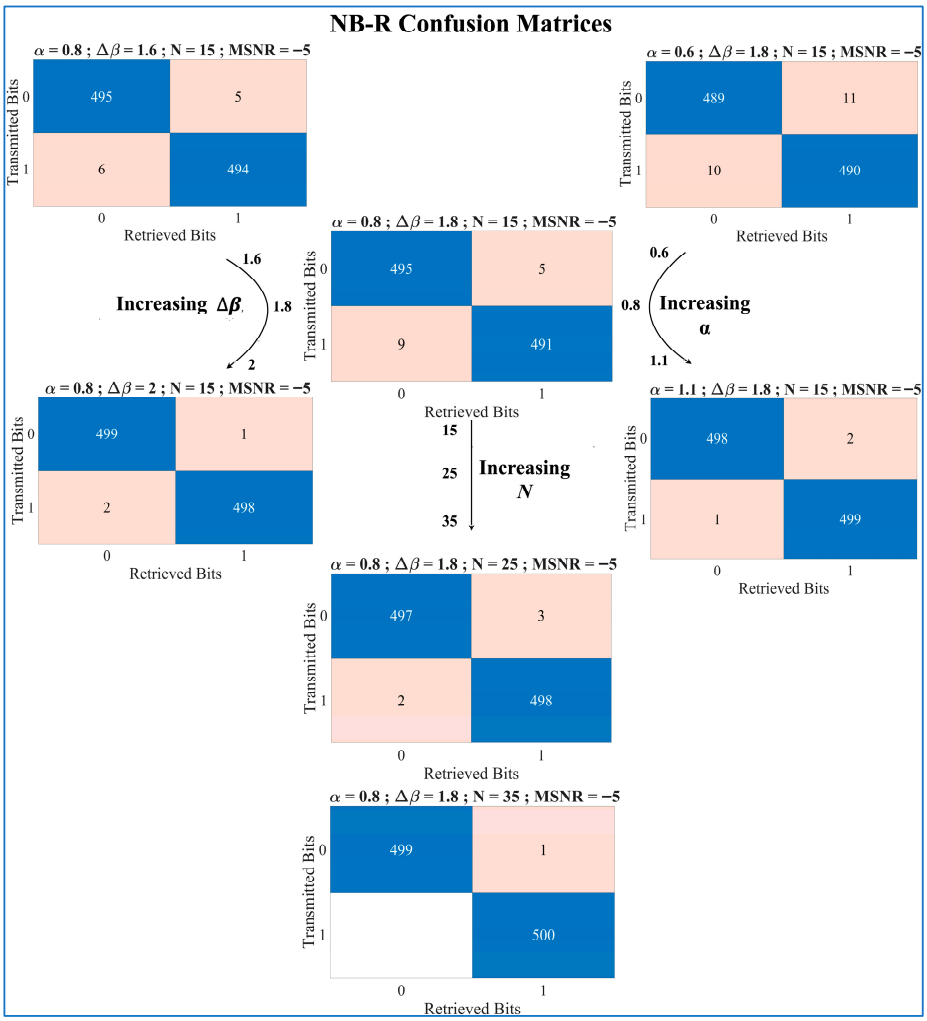



**Figure 3.** Confusion matrices of the NB-R as intended receiver reflecting the individual effects of $\Delta\beta$, $\alpha$, and $N$ on 1000-bit transmission at $\text{MSNR}_{\text{dB}} = -5$ dB. The figure clearly shows optimized decryption while utilizing a higher value combination of the restricted-access keys.

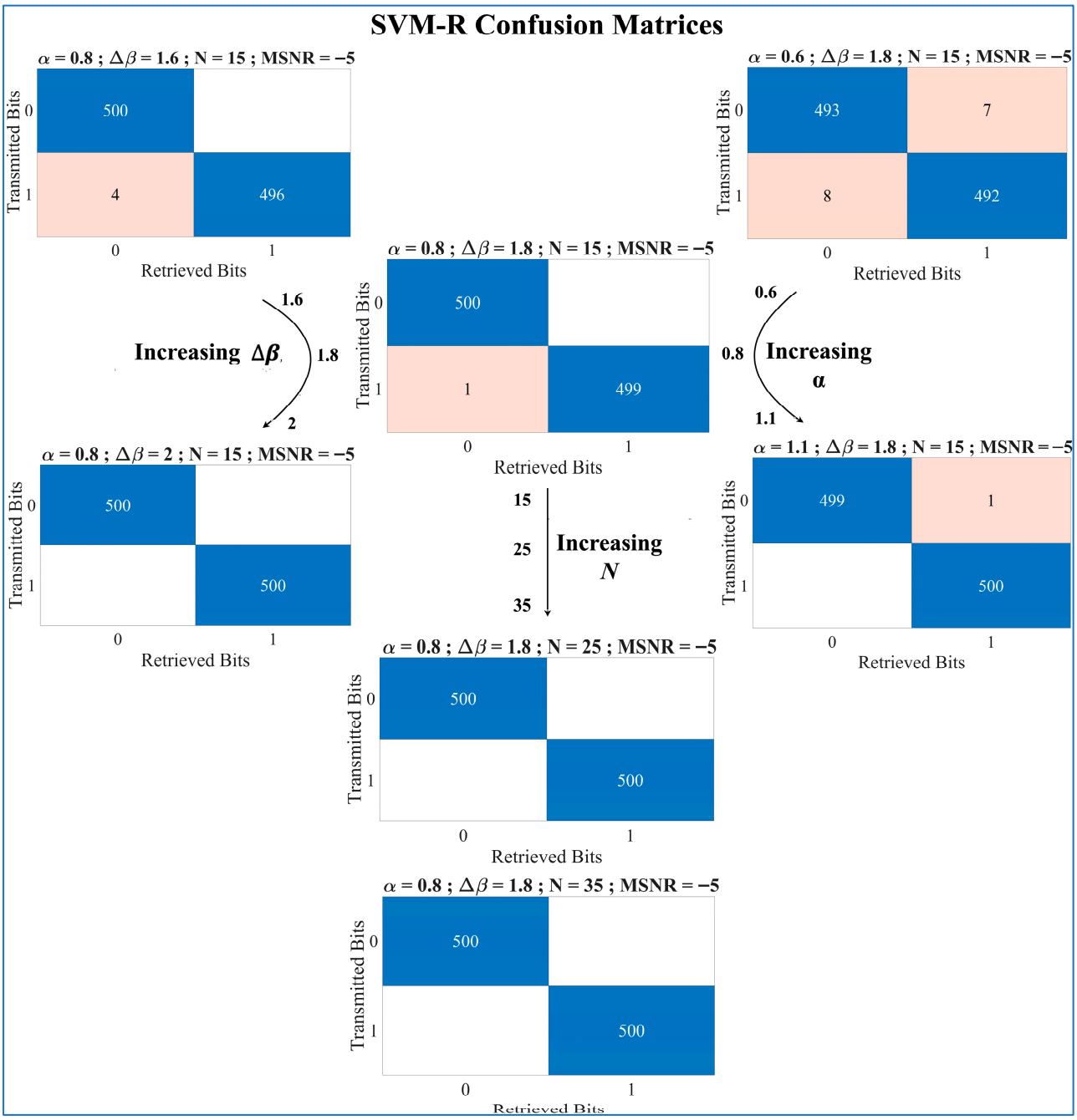



**Figure 4.** Confusion matrices of the SVM-R as intended receiver reflecting the individual effects of $\Delta\beta$, $\alpha$, and $N$ on 1000-bit transmission at $\text{MSNR}_{\text{dB}} = -5$ dB. The figure clearly shows optimized decryption while utilizing a higher value combination of the restricted-access keys.

The confusion matrices of the NB-R in Figure 3 depict the HDR-MLRCS's decryption ability with a fixed channel impairment ($\text{MSNR}_{\text{dB}} = -5$ dB). We observed that all combinations of the restricted-access keys successfully retrieved the binary digits. However, performance continued to increase further when utilizing higher values of $\alpha$, $\Delta\beta$, and $N$.

Like the observation regarding the performance of NB-R in Figure 3, Figure 4 reflects the same trend for SVM-R. The SVM-R's decryption ability tended to increase with the increase in $\alpha$, $\Delta\beta$, and $N$. The SVM-R achieved an ultimate performance of $10^{-3}$, i.e., one out of a thousand bits in error. Moreover, some higher combinations also performed decryption without any errors. The results reflect the HDR-MLRCS's ability to transmit and retrieve binary digits in the restricted-access mode with fixed channel impairment.

#### 4.1.2. Eavesdropper-Receiver

Although the E-R was in no position to decrypt the transmitted binary digits in open-access mode or even detect the presence of communication, we computed confusion matrices for the E-R with the assumption that it knew $\mu = 0$, $\gamma = 1$, $\alpha = 0.8$, and $N = N - 1 = 14$, while only the $\Delta\beta$, the main constituent of the transmitted binary digits, was unknown. With the above assumption and accurate depiction of the best-case scenario for the eavesdropper, we state the E-R confusion matrices for NB-R, DT-R, kNN-R, and SVM-R in Figure 5.

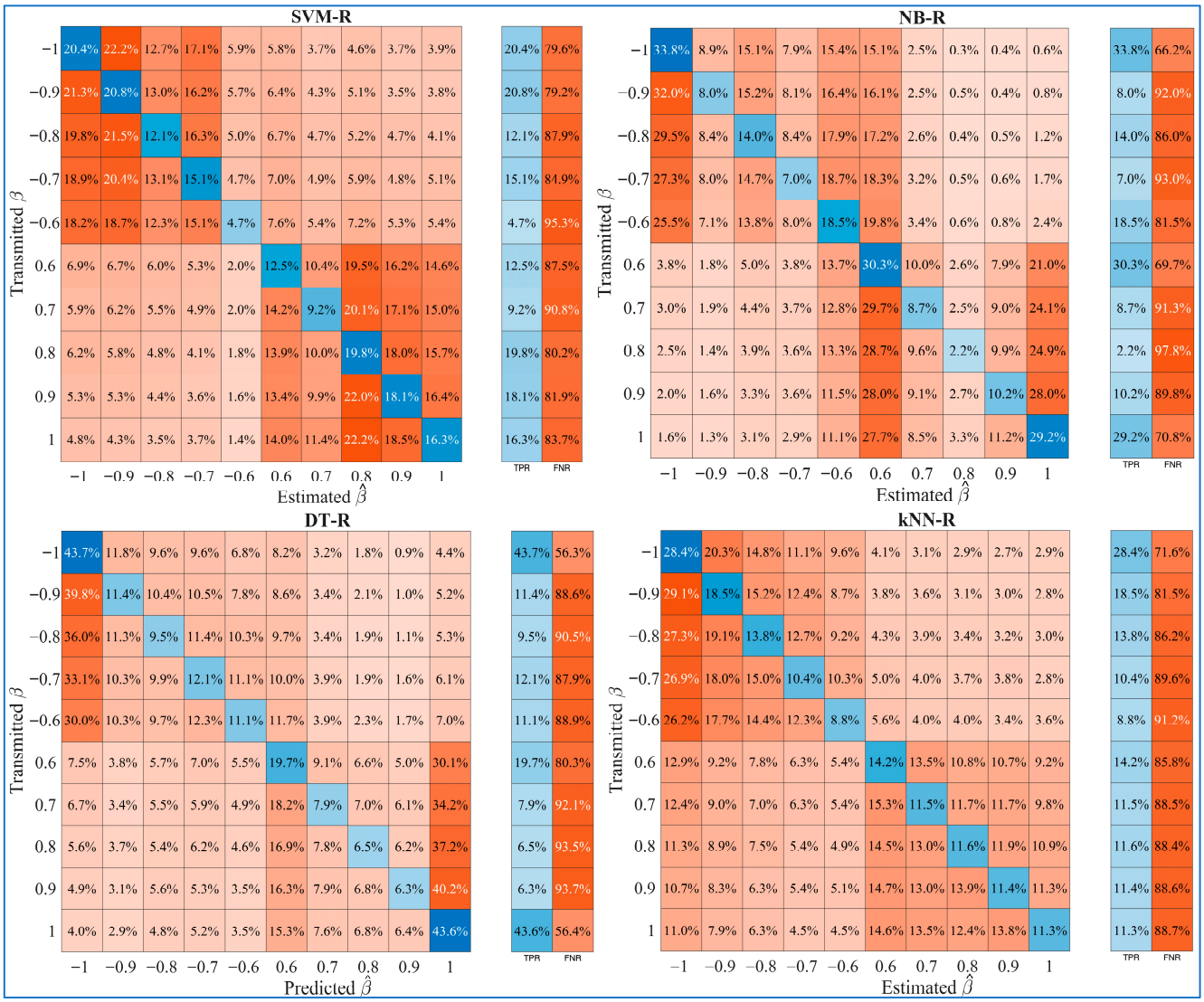



**Figure 5.** Confusion matrices of the E-R (NB-R, DT-R, kNN-R, and SVM-R) reflecting perspectives on potential eavesdropping; $\mu = 0$, $\gamma = 1$, $\alpha = 0.8$, $N = 14$, and $\mathrm{MSNR}_{\mathrm{dB}} = -5$. The inability of E-R to retrieve binary digits is reflected even in its best-case scenario.

We observed that the E-R cannot correctly predict $\hat{\beta}$ even in its most favorable scenario. Even when the RNM and intended receivers are utilizing $\Delta\beta = 2$, the true positive rate (TPR) of E-R for $\hat{\beta}$ did not exceed 30% for NB-R, kNN-R, and SVM-R, and 45% for DT-R. Moreover, the E-R achieved a false negative rate (FNR) above 70% for NB-R, kNN-R, and SVM-R, and 55% for DT-R. The achieved TPR and FNR of the E-R are impractical for retrieving even a single binary digit from the communication occurring in the restricted-

access mode provided by the proposed HDR-MLRCS architecture. This finding indicates that communication is sufficiently secure for the intended purposes.

### *4.2. Bit Error Rate Analysis*

Similarly to the criteria of confusion matrix testing of 1000-bit transmissions, we computed BER vs. $MSNR_{dB}$ graphs in this section to thoroughly analyze the performance of the proposed HDR-MLRCS architecture under various channel impairments.

#### Intended Receivers

Following the trend seen from the confusion matrices of intended receivers, we computed BER vs. $MSNR_{dB}$ plots of all intended receivers, i.e., NB-R, DT-R, kNN-R, and SVM-R in Figures 6 and 7 for all possible combinations of the restricted-access keys.

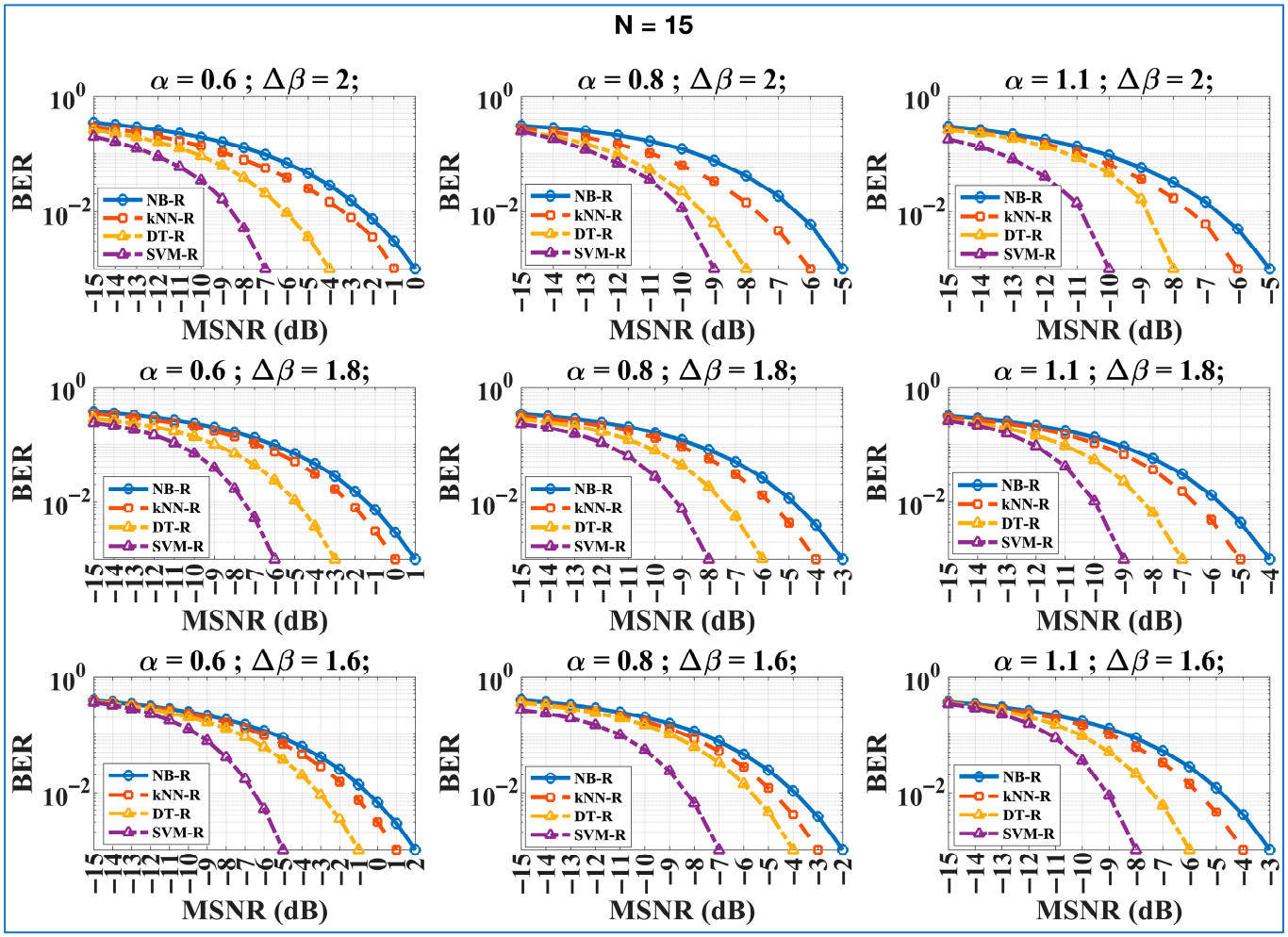



**Figure 6.** BER vs. $MSNR_{dB}$ plots of intended receivers (NB-R, DT-R, kNN-R, and SVM-R) for all possible combinations of $\alpha$ and $\Delta\beta$; $N$ = 15 and total transmitted bits = 1000. Bottom to top: plots with varying $\Delta\beta$ = 1.6, 1.8, 2 with fixed $\alpha$ result in performance increment; left to right: plots with varying $\alpha$ = 0.6, 0.8, 1.1 with fixed $\Delta\beta$ result in performance increment. The figure reflects HDR-MLRCS performance under various channel impairments.

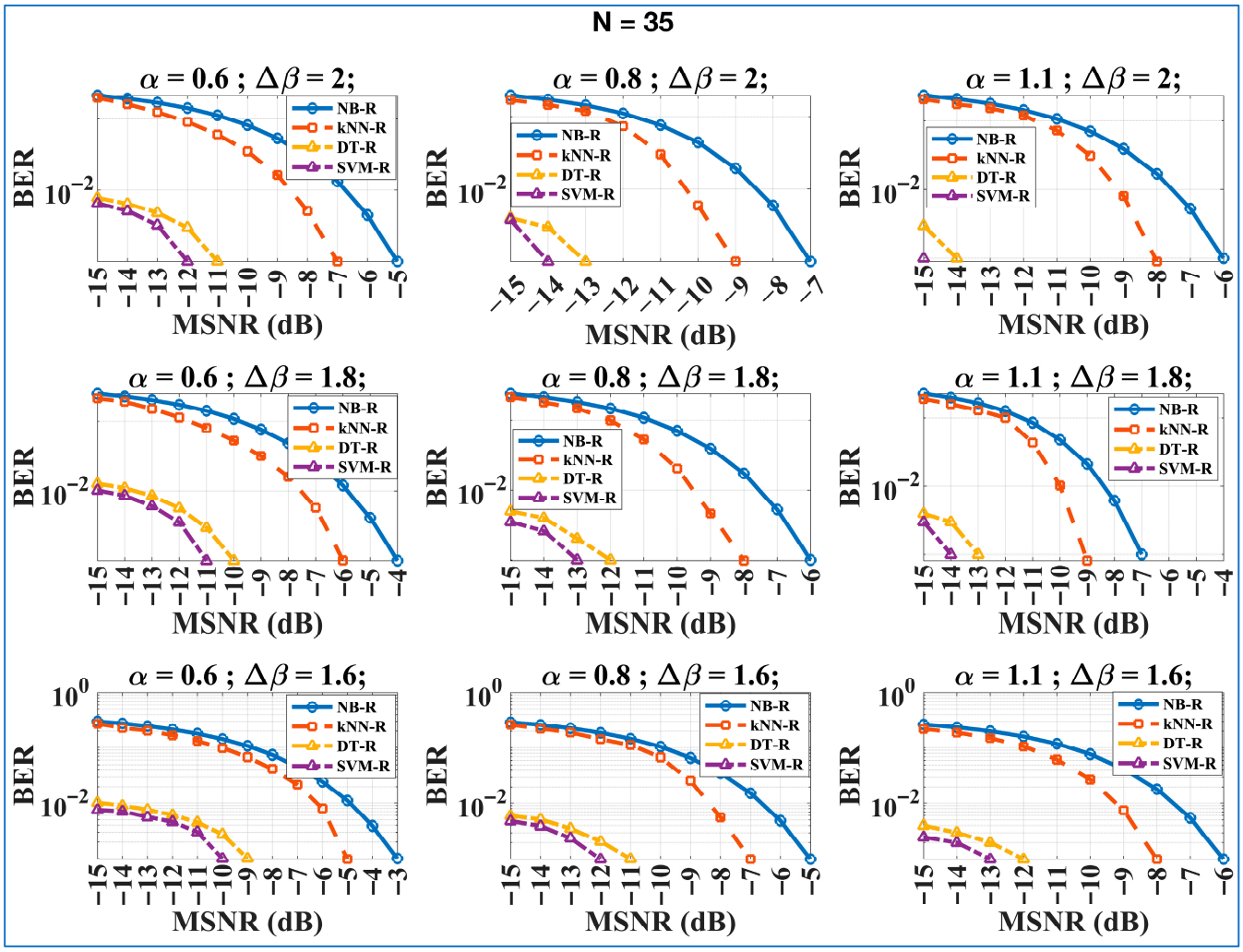



**Figure 7.** BER vs. $MSNR_{dB}$ plots of intended receivers (NB-R, DT-R, kNN-R, and SVM-R) for all possible combinations of $\alpha$ and $\Delta\beta$; $N$ = 35 and total transmitted bits = 1000. Bottom to top: plots with varying $\Delta\beta$ = 1.6, 1.8, 2 with fixed $\alpha$ result in performance increment; left to right: plots with varying $\alpha$ = 0.6, 0.8, 1.1 with fixed $\Delta\beta$ result in performance increment. The figure reflects HDR-MLRCS performance under various channel impairments.

Firstly, in Figure 6, we present the results obtained with $N$ = 15 while varying $\alpha$ and $\Delta\beta$ in all possible combinations. Figure 7 repeats a similar practice for $N$ = 35. In both figures, going from bottom to top, i.e., increasing $\Delta\beta$ from 1.6 to 2, we see a performance increment for all intended receivers. This trend occurred because increasing $\Delta\beta$ increases the difference between $\beta_1$ and $\beta_0$. It ultimately increases the gap between $V_0 \sim S_{\alpha_0}(\beta_0, \gamma, \mu)$ and $V_1 \sim S_{\alpha_1}(\beta_1, \gamma, \mu)$ for transmitted '0' and '1', respectively. The increased dissimilarity between $\beta_1$ and $\beta_0$ makes it easier for intended receivers to accurately decrypt the binary digits as '0' and '1', as per Equation (18).

On the other hand, moving from left to right in both figures, i.e., increasing $\alpha$ from 0.6 to 1.1, we can see a performance improvement for all intended receivers. The main reason is the decreasing difference between the transmitted $\alpha$ utilized in $V_0 \sim S_\alpha(\beta_0, \gamma, \mu)$, $V_1 \sim S_\alpha(\beta_1, \gamma, \mu)$ and the channel impairment $V_G \sim S_{\alpha=2}(\beta = 0, \gamma, \mu)$. This helps the intended receivers correctly predict $\hat{\beta}$ and $\beta_D$ as per Equations (7) and (18), respectively.

We have observed that SVM-R outperforms all other intended receivers under any given combination of restricted-access keys. On the other hand, NB-R lags in every aspect compared to its peers. Similarly, DT-R and kNN-R lie somewhere in between the receivers

for all dynamics. Overall, the derived BER vs. $MSNR_{dB}$ plots of the intended receivers in Figures 6 and 7 reflect that the proposed HDR-MLRCS can achieve the required $10^{-3}$ BER for various combinations of restricted-access keys. It also demonstrates that the HDR-MLRCS architecture can perform effectively under different channel conditions. Moreover, the feasibility of utilizing NB-R, DT-R, kNN-R, and SVM-R as intended receivers further reflects the variation provided by the secure architecture.

We have observed that SVM-R achieves the best accuracy among all intended receivers; kernel optimization and iterative training increase its computational cost. On the contrary, DT-R and kNN-R are more suitable for real-time low-power dynamics. The HDR-MLRCS offers an optional trade-off between faster inference with modest accuracy in a unified architecture.

### *4.3. Data Rate Comparison*

The proposed unified architecture, HDR-MLRCS, provides efficient BER performance against various channel impairments and ensures the security of established communication through its unconventional mechanism. However, its primary significance lies in the achieved data rate compared to previously proposed unconventional RCSs. We conducted a brief comparative analysis of the performance and data rate achieved through HDR-MLRCS compared to previously reported RCSs. The performance dominance of the HDR-MLRCS is shown by analyzing the BERs of all designs. Similarly, we examined the achieved data rates by the number of noise samples (pulse length '$N$') needed to encrypt and decrypt a single binary digit. The sampling conditions were similar to those adopted in previous studies in the literature, i.e., the method given in [36]. We have provided the comparative analysis in Table 4 for approximately the same simulation parameters.

**Table 4.** Comparative analysis.

| Architectures | $MSNR_{dB}$ at BER = $10^{-3}$ | Pulse Length $N$ |
|---|---|---|
| Cek, M.E. [20] | −6 | 2000 |
| Xu et al. [21] | −12 | 2000 |
| Savaci et al. [22] | −5 | 1000 |
| Ahmed et al. [23] | −4 | 1000 |
| Cek, M.E. [24] | −6 | 1600 |
| Ahmed et al. [25] | −5 | 500 |
| NB-R | −5; −6 | 15; 35 |
| kNN-R | −6; −8 | 15; 35 |
| DT-R | −8; −14 | 15; 35 |
| SVM-R | −10; −15 | 15; 35 |

- A lower $MSNR_{dB}$ reflects a very severe presence of AWGN and vice versa. The comparative analysis reflects that the proposed HDR-MLRCS can achieve the ideal BER of $10^{-3}$ in very harsh channel conditions. Moreover, the architecture provides the feasibility of achieving it with all intended receivers. The achievement of BER = $10^{-3}$ at the $MSNR_{dB}$ = −15 by SVM-R specifically portrays the lowest possible value among all RCS architectures.
- Similarly, achieving the ideal BER by NB-R, kNN, and DT-R at the lowest $MSNR_{dB}$ values demonstrates the robustness of the HDR-MLRCS in establishing and maintaining secure communications under severe channel impairments.
- Most importantly, we can attain this level of performance with $N$ = 15 and $N$ = 35 at lower $MSNR_{dB}$ values. It follows that the proposed HDR-MLRCS can securely transmit one binary digit with only 15 noise samples. In contrast, the closest architectures require 500 to 2000 samples to do this. This reflects that the unified architecture

can transmit approximately ($\frac{500}{15}$ = 33 to $\frac{2000}{15}$ = 133) more bits, in one time duration, compared to all previous architectures.

Such high data rates reflect the HDR-MLRCS's supremacy over other unconventional RCS architectures and highlight its potential to compete with conventional communication systems. It also makes SVM-R the optimal choice among other peers.

## 5. Conclusions

We modified the concept of random communication systems by incorporating various baseline ML algorithms to encrypt and decrypt $\alpha$-stable noise carriers. The proposed HDR-MLRCS systematically integrates several ML algorithms—SVM, NB, DT, and kNN—as intended receivers. We successfully achieved the target of establishing secure communication with efficient BER performance under harsh channel environments. The Monte Carlo simulation results demonstrate that the deployment of ML-based receivers was the reason behind the enhanced BER performance and decryption. Most importantly, the proposed HDR-MLRCS produced significantly boosted data rates compared to previous RCS architectures. It also reflects the proposed unified architecture's ability to compete with conventional carrier-based communication systems.

By exploiting the individual classification ability of various ML classifiers, the HDR-MLRCS achieved higher adaptability to channel impairments and increased resistance against eavesdropping, reinforcing physical layer security. Following the evolutionary path of RCS architectures, we established baseline performance metrics to use in AWGN environments. We extend HDR-MLRCS to Rayleigh–Rician fading channels when channel characteristics or pulse length are highly variable. Moreover, utilizing advanced algorithms such as deep learning-based alternatives and transfer learning to create complex decision boundaries with improved generalization is a concern in ongoing studies. We also plan to implement the proposed HDR-MLRC architecture on software-defined radios and field programmable gate arrays for real-world performance validation under measured $\alpha$-stable noise channels. In parallel to the above directions, we are conducting a separate study on the relation between runtime behavior and computational complexity of adversarial ML-driven receivers under broader $\alpha$-stable datasets of different sizes, biases, and parameters. It will explore quantitative comparison for various disciplines utilizing $\alpha$-stable noise for versatile edge-case purposes. Following the above-discussed future research pathways, we plan to transform the 5G/6G systems and explore more resilient, adaptive, fast, and secure communication infrastructures.

**Author Contributions:** Conceptualization, A.A.; methodology, A.A.; software, A.A.; validation, Z.B.; formal analysis, A.A.; investigation, A.A.; resources, Z.B.; data curation, A.A.; writing—original draft, A.A.; writing—review and editing, Z.B.; visualization, A.A.; supervision, Z.B.; project administration, Z.B.; funding acquisition, Z.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This publication is supported by the European Union's Horizon Europe research and innovation program under the Marie Skłodowska-Curie Postdoctoral Fellowship Programme, cofunded by SMASH under grant agreement No. 101081355.

**Data Availability Statement:** The raw data supporting the conclusions of this article will be made available by the authors on request.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| HDR-MLRCS | High-Data-Rate Machine-Learning-Driven Secure Random Communication System |
| AWGN | Additive White Gaussian Noise |
| RCS | Random Communication System |
| BER | Bit Error Rate |
| $MSNR_{dB}$ | Mixed Signal-to-Noise Ratio |
| RNM | Random Noise Modulator |
| ML | Machine Learning |
| 5G/6G | Fifth Generation/Sixth Generation |
| SVM-R | Support Vector Machine-Aided Receiver |
| NB-R | Naïve Bayes-Aided Receiver |
| kNN-R | k-Nearest Neighborhood-Aided Receiver |
| DT-R | Decision Tree-Aided Receiver |

## References


1. Balendran, A.; Beji, C.; Bouvier, F.; Khalifa, O.; Evgeniou, T.; Ravaud, P.; Porcher, R. A scoping review of robustness concepts for machine learning in healthcare. *npj Digit. Med.* **2025**, *8*, 38. [CrossRef]
2. Guidotti, D.; Pandolfo, L.; Pulina, L. A systematic literature review of supervised machine learning techniques for predictive maintenance in Industry 4.0. *IEEE Access* **2025**, *13*, 102479–102504. [CrossRef]
3. Rizvi, S.M.A.; Paracha, U.I.; Khalid, U.; Lee, K.; Shin, H. Quantum Machine Learning: Towards Hybrid Quantum–Classical Vision Models. *Mathematics* **2025**, *13*, 2645. [CrossRef]
4. Damjanović, D.; Biočić, P.; Prakljačić, S.; Činčurak, D.; Balen, J. A comprehensive survey on SLAM and machine learning approaches for indoor autonomous navigation of mobile robots. *Mach. Vis. Appl.* **2025**, *36*, 55. [CrossRef]
5. Dritsas, E.; Trigka, M. Machine Learning in Information and Communications Technology: A Survey. *Information* **2024**, *16*, 8. [CrossRef]
6. Celik, A.M.; Eltawil, A. At the dawn of generative AI era: A tutorial-cum-survey on new frontiers in 6G wireless intelligence. *IEEE Open J. Commun. Soc.* **2024**, *5*, 2433–2489. [CrossRef]
7. He, H.; Wen, C.; Jin, S.; Li, G.Y. Model-driven deep learning for MIMO detection. *IEEE Trans. Signal Process.* **2020**, *68*, 1702–1715. [CrossRef]
8. Marin Machado de Souza, R.; Holm, A.; Biczyk, M.; de Castro, L.N. A systematic literature review on the use of federated learning and bioinspired computing. *Electronics* **2024**, *13*, 3157. [CrossRef]
9. Weththasinghe, K.; Rajatheva, N.; He, Y. Machine learning-based channel estimation for 5G new radio. *IEEE Wirel. Commun. Lett.* **2024**, *13*, 1133–1137. [CrossRef]
10. Kee, H.L.M.; Ong, L.C.; Tan, W.H.; Teo, K.T.K. A review on machine learning for channel coding. *IEEE Access* **2024**, *12*, 89002–89025. [CrossRef]
11. Elsadig, A.; Gafar, A. Covert channel detection: Machine learning approaches. *IEEE Access* **2022**, *10*, 38391–38405. [CrossRef]
12. Gebrezgiher, Y.T.; Jeremiah, S.R.; Deng, X.; Park, J.H. Machine Learning-Based Blockchain Technology for Secure V2X Communication: Open Challenges and Solutions. *Sensors* **2025**, *25*, 4793. [CrossRef] [PubMed]
13. Pan, S.; Yin, L.; Tan, Y.; Wang, Y. Structure Design and Reliable Acquisition of Burst Spread Spectrum Signals Without Physical Layer Synchronization Overhead. *Electronics* **2024**, *13*, 4586. [CrossRef]
14. Guan, H.; Fu, J.; Li, B.; Wei, H.; Jiang, P.; Zhao, S.; Huang, Y. Research on Direct Spread Spectrum Signal Monitoring Technology Based on Combined Partitioned Matched Filter–Fast Fourier Transform and Partitioned Matched Filter–Fractional Fourier Transform Algorithms. *Appl. Sci.* **2025**, *15*, 8958. [CrossRef]
15. Dinu, A.; Frunzete, M. Image Encryption Using Chaotic Maps: Development, Application, and Analysis. *Mathematics* **2025**, *13*, 2588. [CrossRef]
16. Eltholth, A.A. Improved spectrum coexistence in 2.4 GHz ISM band using optimized chaotic frequency hopping for WiFi and Bluetooth signals. *Sensors* **2023**, *23*, 5183. [CrossRef]
17. Mushenko, A.; Pakulova, E.; Basan, E.; Nekrasov, A.; Gamcová, M.; Kurdel, P. Modeling a single-channel synergetic observer for chaos-based secure communication system applications. *Mathematics* **2024**, *12*, 2764. [CrossRef]
18. Gu, C.; Cao, X. Research on information hiding technology. In Proceedings of the International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 21–23 April 2012; pp. 2035–2037. [CrossRef]

19. Ahmed, A.; Savaci, F.A. Structure and performance evaluation of fractional lower-order covariance method in alpha-stable noise environments. *Recent Adv. Electr. Electron. Eng.* **2019**, *12*, 40–44. [CrossRef]
20. Cek, M.E.; Savaci, F.A. Stable non-Gaussian noise parameter modulation in digital communication. *Electron. Lett.* **2009**, *45*, 1256–1257. [CrossRef]
21. Xu, Z.; Jin, W.; Zhou, K.; Hua, J. A covert digital communication system using skewed $\alpha$-stable distributions for Internet of Things. *IEEE Access* **2020**, *8*, 113131–113141. [CrossRef]
22. Savaci, F.A.; Ahmed, A. Inverse system approach to design alpha-stable noise-driven random communication systems. *IET Commun.* **2020**, *14*, 910–913. [CrossRef]
23. Ahmed, A.; Bosnić, Z. A covert $\alpha$-stable noise-based extended random communication by incorporating multiple inverse systems. *IEEE Access* **2025**, *13*, 13675–13685. [CrossRef]
24. Cek, M.E. M-ary alpha-stable noise modulation in spread-spectrum communication. *Fluct. Noise Lett.* **2015**, *14*, 1550022. [CrossRef]
25. Ahmed, A.; Savaci, F.A. Covert electromagnetic nanoscale communication system in the terahertz channel. *J. Circuits Syst. Comput.* **2020**, *29*, 2050126. [CrossRef]
26. Fang, H.; Wang, X.; Hanzo, L. Learning-aided physical layer authentication as an intelligent process. *IEEE Trans. Commun.* **2019**, *67*, 2260–2273. [CrossRef]
27. Saleem, J.; Raza, U.; Hammoudeh, M.; Holderbaum, W. Machine Learning-Enhanced Attribute-Based Authentication for Secure IoT Access Control. *Sensors* **2025**, *25*, 2779. [CrossRef]
28. Alsalman, D. A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats. *IEEE Access* **2024**, *12*, 14719–14730. [CrossRef]
29. Wang, Z.; Wang, Y.; Xiong, X.; Ren, Q.; Huang, J. A Novel Framework for Enhancing Decision-Making in Autonomous Cyber Defense Through Graph Embedding. *Entropy* **2025**, *27*, 622. [CrossRef] [PubMed]
30. Natarajan, A.; Krishnasamy, V.; Singh, M. Device-Free Human Activity Recognition in Through-the-Wall Scenarios using Single Link WiFi Channel Measurements. *IEEE Sens. J.* **2025**, *25*, 14. [CrossRef]
31. Akram, U.; Sharif, W.; Shahroz, M.; Mushtaq, M.F.; Aray, D.G.; Thompson, E.B.; Diez, I.d.l.T.; Djuraev, S.; Ashraf, I. IoTTPS: Ensemble RKSVM model-based Internet of Things threat protection system. *Sensors* **2023**, *23*, 6379. [CrossRef] [PubMed]
32. Noor, K.; Imoize, A.L.; Li, C.T.; Weng, C.Y. A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond. *Mathematics* **2025**, *13*, 1088. [CrossRef]
33. Zhang, Y.; Zhang, Y. An adaptive parameter estimation algorithm of radar linear frequency modulation signal based on nonlinear transform under different $\alpha$-stable distribution noise environments. *IEEE J. Miniatur. Air Space Syst.* **2023**, *4*, 389–399. [CrossRef]
34. Peppas, K.P.; Mathiopoulos, P.T. Space shift keying (SSK) transmission over Rayleigh fading channels and symmetric $\alpha$-stable noise. *IEEE Access* **2024**, *12*, 40569–40581. [CrossRef]
35. Zhang, J.; Li, X.; Wang, Y.; Chen, Y. Multiantenna spectrum sensing with $\alpha$-stable noise for cognitive radio-enabled IoT. *IEEE Internet Things J.* **2024**, *11*, 12. [CrossRef]
36. Samorodnitsky, G.; Taqqu, M.S. *Stable Non-Gaussian Random Processes*; Chapman & Hall/CRC: New York, NY, USA, 1994; pp. 23–45. [CrossRef]


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.